KASPERSKY LAB

Kaspersky® Internet Security 7.0

MANUALE DELL'UTENTE

KASPERSKY INTERNET SECURITY 7.0

Manuale dell'utente

http://www.kaspersky.it

Data di revisione: Febbraio 2008

Sommario

CAPITOLO 1. LE MINACCE ALLA SICUREZZA DEL COMPUTER

Poiché la tecnologia informatica si è sviluppata rapidamente penetrando in ogni aspetto dell'esistenza umana, la quantità di azioni illecite volte a minare la sicurezza delle informazioni si è moltiplicata.

I criminali informatici hanno mostrato un profondo interesse nelle attività di strutture governative e imprese commerciali. Essi cercano di impadronirsi di e diffondere informazioni riservate, danneggiando la reputazione di imprese, interrompendo la continuità di attività commerciali e, di conseguenza, violando le risorse informative di organizzazioni. Questi atti possono recare gravi danni a beni materiali e immateriali.

Ma non sono solo le grandi aziende a correre rischi. Anche gli utenti privati possono cadere vittima degli attacchi informatici. Servendosi di vari strumenti, i criminali accedono ai dati personali (numero di conto corrente e carta di credito, password, ecc.), provocano anomalie di funzionamento del sistema o ottengono l'accesso completo a computer altrui. Quei computer possono quindi essere utilizzati come elementi di una rete "zombie", cioè una rete di computer infetti usati dagli hacker per attaccare server, inviare spam, impadronirsi di informazioni riservate e diffondere nuovi virus e troiani.

Oggigiorno chiunque riconosce il valore dell'informazione ed è consapevole della necessità di proteggere i dati. Al tempo stesso l'informazione deve essere facilmente accessibile a determinati gruppi di utenti (per esempio dipendenti, clienti e partner di un'impresa). Ecco perché è necessario realizzare un vasto sistema di protezione dei dati. Questo sistema deve tenere conto di tutte le possibili minacce, siano esse umane, prodotte dall'uomo o conseguenze di catastrofi naturali, e applicare una serie completa di misure protettive a livello fisico, amministrativo e di software.

1.1. Origine delle minacce

Singole persone, gruppi di persone o perfino fenomeni non correlati ad attività umane rappresentano potenziali minacce per la sicurezza dei dati. Le minacce potenziali possono essere suddivise in tre categorie:

- **Fattore umano.** Questo gruppo riguarda le azioni di persone autorizzate o non autorizzate ad accedere ai dati. Le minacce di questo gruppo possono essere:
  - *Esterne*: criminali informatici, hacker, truffe via internet, partner sleali e organizzazioni criminali.
  - *Interne:* azioni del personale di un'azienda e degli utenti di PC ad uso domestico. Le azioni di questo gruppo possono essere deliberate o accidentali.
- **Fattore tecnologico**. Questo gruppo si riferisce a problemi tecnici: apparecchiature obsolete o software e hardware di scarsa qualità utilizzati per l'elaborazione delle informazioni. Questi fattori determinano il malfunzionamento delle apparecchiature e frequenti perdite di dati.
- **Fattore naturale**. Questo gruppo include qualsiasi evento naturale o altri eventi non dipendenti dall'attività dell'uomo.

Un sistema di protezione dati efficiente deve tener conto di tutti questi fattori. Questo manuale d'uso si riferisce esclusivamente a quelli di competenza diretta di Kaspersky Lab: le minacce esterne derivanti da attività umana.

1.2. La diffusione delle minacce

Man mano che la moderna tecnologia informatica e gli strumenti di comunicazione si evolvono, gli hacker possono contare su un numero crescente di opportunità per diffondere le loro minacce. Osserviamole più da vicino:

Internet

La rete Internet è unica in quanto non appartiene a nessuno e non è delimitata da confini geografici. Essa ha contribuito in molti modi allo sviluppo di innumerevoli risorse di rete e allo scambio di informazioni. Oggi tutti possono accedere ai dati disponibili su Internet o creare la propria pagina web.

Tuttavia proprio queste caratteristiche della rete offrono agli hacker la possibilità di commettere crimini via Internet, spesso senza essere individuati e puniti.

Gli hacker infettano i siti Internet con virus e altri programmi maligni facendoli passare come utili applicazioni gratuite (freeware). Inoltre gli script eseguiti automaticamente all'apertura di una pagina web sono in grado di eseguire azioni pericolose sul computer, fra cui la modifica del registro di sistema, il furto di dati personali e l'installazione di software nocivi.

Grazie alle tecnologie di rete, gli hacker possono attaccare PC e server aziendali remoti. Questi attacchi possono provocare il malfunzionamento di

parte del sistema o fornire agli hacker l'accesso completo al sistema stesso e alle informazioni in esso memorizzate. Il sistema può essere utilizzato anche come elemento di una rete "zombie".

Da quando è stato reso possibile l'uso delle carte di credito e di moneta elettronica su Internet per acquisti su negozi online, aste e pagine web di istituti di credito, le truffe online sono diventate uno dei crimini maggiormente diffusi.

Intranet

Intranet è una rete interna progettata specificamente per gestire le informazioni nell'ambito di un'azienda o di una rete domestica. Si tratta di uno spazio unificato per a cui tutti i computer della rete possono accedere per memorizzare, scambiare e consultare dati. Ciò significa che se un computer di tale rete è infetto, anche tutti gli altri corrono un grave rischio di infezione. Al fine di evitare una tale situazione, sia il perimetro della rete sia ogni singolo computer devono essere protetti.

E-mail

Poiché quasi tutti i computer hanno un client di posta elettronica installato e i programmi nocivi sfruttano i contenuti delle rubriche elettroniche, la diffusione di programmi nocivi può contare su condizioni ottimali. È possibile che l'utente di un computer infetto, ignaro di quanto sta avvenendo, invii e-mail infette ad amici e colleghi che, a loro volta, diffondono l'infezione. È molto comune che documenti infetti non individuati vengano inviati trasmettendo informazioni relative a grandi aziende. Quando ciò avviene, sono molti gli utenti che vengono infettati. Può trattarsi di centinaia o migliaia di persone che, a loro volta, inviano i file infetti a decine di migliaia di utenti.

Oltre alla minaccia dei programmi nocivi esiste quella della posta indesiderata, o spam. Sebbene questa non rappresenti una minaccia diretta per il computer, lo spam incrementa il carico sui server di posta, consuma larghezza di banda, riempie caselle elettroniche e determina la perdita di ore lavorative, provocando danni finanziari.

Gli hacker, inoltre, hanno iniziato a fare uso di programmi di mass mailing e di tecniche di social engineering per convincere gli utenti ad aprire messaggi e-mail o a fare clic su un determinato sito web. Le funzionalità di filtro antispam, di conseguenza, oltre a contrastare la posta spazzatura e i nuovi tipi di scansione online come il phishing, contribuiscono ad ostacolare la diffusione dei programmi nocivi.

Supporti di archiviazione esterni

I supporti esterni (floppy, CD-ROM e flash drive USB) sono molto usati per l'archiviazione e la trasmissione di informazioni.

All'apertura di un file contenente un codice maligno da un supporto di archiviazione esterno, è possibile che i file conservati nel computer si

infettino diffondendo il virus a tutte le altre unità del computer o agli altri computer della rete.

1.3. Tipi di minacce

Oggigiorno esistono numerosi tipi di minaccia che potrebbero pregiudicare il funzionamento di un computer. Questa sezione esamina le minacce bloccate da Kaspersky Internet Security.

Worm

Questa categoria di programmi nocivi si diffonde sfruttando in gran parte le vulnerabilità del sistema. Essi devono il loro nome alla capacità di "strisciare" come i vermi da un computer all'altro attraverso reti, posta elettronica e altri canali di informazione. Questa caratteristica consente ai worm di diffondersi con una velocità piuttosto elevata.

I worm penetrano all'interno di un computer, calcolano gli indirizzi di rete di altri computer e inviano loro una quantità di repliche di se stessi. Oltre agli indirizzi di rete, i worm utilizzano spesso i dati contenuti nelle rubriche dei client di posta elettronica. Alcuni di questi programmi maligni creano di quando in quando dei file di lavoro sui dischi di sistema, ma riescono a funzionare senza alcuna risorsa ad eccezione della RAM.

Virus

Programmi che infettano altri programmi aggiungendovi il proprio codice al fine di ottenere il controllo non appena un file infetto viene eseguito. Questa semplice definizione spiega il principio alla base della diffusione di un virus: l'*infezione*.

Trojan

Programmi che eseguono azioni non autorizzate, per esempio la cancellazione di dati sui drive provocando il blocco del sistema, il furto di informazioni confidenziali, ecc. Questa categoria di programmi nocivi non può essere definita virus nel senso tradizionale del termine in quanto non infetta altri computer o dati. I trojan non sono in grado di penetrare autonomamente in un computer ma vengono diffusi dagli hacker che li fanno passare per software regolare. I danni provocati dai trojan possono essere notevolmente superiori a quelli dei virus tradizionali.

Di recente, la categoria di programmi nocivi maggiormente diffusa è stata quella dei worm, seguita da virus e troiani. Alcuni programmi nocivi combinano le caratteristiche di due o addirittura tre di queste categorie.

Adware

L'Adware è un codice di programma incluso nel software, all'insaputa dell'utente, progettato per visualizzare messaggi pubblicitari. L'adware è solitamente incorporato nel software a distribuzione gratuita e il messaggio è situato nell'interfaccia del programma. Questi programmi spesso raccolgono anche dati personali relativi all'utente e li inviano allo sviluppatore, modificano le impostazioni del browser (pagina iniziale e pagine di ricerca, livello di sicurezza, ecc.) e creano un traffico che l'utente non è in grado di controllare. Tutto ciò può provocare la violazione delle regole di sicurezza e, in ultima analisi, perdite finanziarie.

Spyware

Lo Spyware è un software che raccoglie informazioni su un utente o azienda a loro insaputa. Talvolta esso si installa in un computer senza che l'utente se ne accorga. In generale gli obiettivi dello spyware sono:

- Ricostruire le azioni dell'utente su un computer.
- Raccogliere informazioni sui contenuti del disco fisso; in tal caso, ciò comporta quasi sempre la scansione di numerose directory e del registro di sistema al fine di compilare un elenco dei software installati sul computer.
- Raccogliere informazioni sulla qualità della connessione, larghezza di banda, velocità del modem, ecc.

Riskware

Software potenzialmente rischioso che non svolge una funzione nociva vera e propria ma che può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. In determinate condizioni, la presenza di tali programmi nel computer rappresenta una fonte di rischio per i proprio dati. Questi programmi includono, per esempio, alcune utilità di amministrazione remota, commutatori di tastiera, client IRC, server FTP e utilità multifunzione per interrompere processi o per nasconderne il funzionamento.

Esiste un altro tipo di programma nocivo trasmesso con adware, spyware e riskware: sono quei programmi che penetrano nel web browser e reindirizzano il traffico. Chiunque abbia avuto l'esperienza di aprire un sito web credendo di caricarne uno diverso, quasi certamente ha incontrato uno di questi programmi.

Joke

Software che non reca alcun danno diretto ma visualizza messaggi secondo i quali il danno è già stato provocato o lo sarà in circostanze particolari. Questi programmi spesso comunicano all'utente la presenza di rischi inesistenti, per esempio sulla formattazione del disco fisso (anche se non ha luogo alcuna formattazione) o l'individuazione di virus in file non infetti.

Rootkit

Utilità che celano attività nocive. Esse nascondono programmi nocivi che impediscono agli antivirus di individuarli. I rootkit modificano il sistema operativo del computer e ne alterano le funzioni di base per nascondere la propria esistenza e le azioni intraprese dagli hacker sul computer infetto.

Altri programmi pericolosi

Programmi creati per lanciare attacchi Dos su server remoti e penetrare in altri computer, e programmi che fanno parte dell'ambiente di sviluppo dei programmi nocivi. Essi includono hack tool, virus builder, scanner di vulnerabilità, programmi di individuazione di password, e altri tipi di programma per penetrare in un sistema o utilizzare risorse di rete.

Attacchi di pirateria informatica

Gli attacchi di pirateria informatica possono essere avviati da hacker o da programmi nocivi. Essi hanno lo scopo di sottrarre informazioni da un computer remoto provocando il malfunzionamento del sistema, oppure di ottenere il controllo completo delle risorse del computer. Per una descrizione dettagliata degli usi della rete, vedi 12.1.3 a pag. 177.

Alcuni tipi di truffe online

Il **"phishing"** è una truffa online che impiega il mass mailing per carpire informazioni confidenziali, solitamente di natura confidenziale, sugli utenti. I messaggi inviati a tal fine sono concepiti in modo da indurre a credere che si tratti di e-mail informative da parte di istituti di credito e note aziende. Contengono dei link che aprono siti contraffatti, realizzati dagli hacker in modo da riprodurre il sito ufficiale dell'organizzazione che fingono di rappresentare. Il sito richiede all'utente di digitare, per esempio, il numero della carta di credito e altre informazioni confidenziali.

Dialer per siti a pagamento – tipo di truffa online basata sull'uso non autorizzato di servizi Internet a pagamento (solitamente siti web con contenuti pornografici). I dialer installati dagli hacker stabiliscono il contatto via modem tra il computer colpito e il numero telefonico del servizio a pagamento. Si tratta frequentemente di numeri con tariffe molto elevate che costringono l'ignaro utente al pagamento di bollette telefoniche costosissime.

Messaggi pubblicitari importuni

Ne fanno parte le finestre a comparsa (popup) e i banner pubblicitari che si aprono durante la navigazione. Le informazioni contenute in tali finestre di solito non sono di alcun interesse per il navigatore comune. I popup e i banner distraggono l'utente dall'occupazione che stava svolgendo e consumano larghezza di banda.

Spam

Lo spam è posta "spazzatura" anonima, che comprende marketing, messaggi di natura politica e provocatoria o richieste di assistenza. Un'altra categoria di spam è costituita da proposte di investire ingenti somme di denaro o di entrare a far parte di strutture piramidali, e-mail volte a carpire password e numeri di carte di credito, e e-mail da trasmettere ad amici (catene di Sant'Antonio).

Lo spam aumenta significativamente il carico sui server di posta e il rischio di perdita di dati importanti.

Kaspersky Internet Security adotta due metodi per individuare e bloccare questi tipi di minaccia:

- *Metodi reattivi* – basati sulla ricerca di file nocivi per mezzo di database delle firme regolarmente aggiornati. Questo metodo richiede l'inserimento delle firme coinvolte nel database e lo scaricamento degli aggiornamenti.
- *Metodi proattivi* – contrariamente ai metodi reattivi, non si basano sull'analisi di codici ma del comportamento del sistema. Questi metodi sono finalizzati all'individuazione di nuove minacce non ancora definite nelle firme.

Grazie all'applicazione di entrambi i metodi, Kaspersky Internet Security garantisce una protezione completa del computer contro le minacce già note e quelle ancora ignote.

Attenzione!

Da questo momento, sarà utilizzato il termine "virus" per fare riferimento sia ai programmi nocivi che pericolosi. Il tipo di programma nocivo sarà sottolineato solo se necessario.

1.4. Segnali di infezione

Vi sono numerosi segnali che indicano la presenza di un virus all'interno del computer. Di solito il computer si comporta in maniera strana, in particolare:

- Il video visualizza messaggi o immagini impreviste, oppure il computer emette suoni anomali;
- Il lettore CD/DVD-ROM si apre e si chiude inaspettatamente;
- Il computer apre arbitrariamente un programma non richiesto dall'utente;
- Il video visualizza messaggi pop up che informano che un determinato programma nel computer sta cercando di accedere a Internet, anche se tale azione non è stata richiesta dall'utente.

In tutti questi casi è molto probabile che il computer sia infetto da un virus.

Anche l'infezione attraverso la posta elettronica presenta numerosi tratti caratteristici:

- Amici e parenti sostengono di aver ricevuto messaggi che l'utente non ha mai inviato;
- La casella di posta elettronica contiene numerosi messaggi privi di mittente o intestazione.

Occorre specificare che questi segnali possono anche essere il risultato di problemi diversi dai virus. Talvolta hanno effettivamente altre cause. Per esempio, nel caso della posta elettronica, è possibile che i messaggi infetti vengano inviati con l'indirizzo di un mittente specifico ma non dal suo computer.

Vi sono anche sintomi indiretti che indicano una probabile infezione del computer:

- Il computer si blocca o ha crash frequenti.
- Il computer carica i programmi con eccessiva lentezza.
- Non si riesce a inizializzare il sistema operativo.
- File e cartelle scompaiono o i loro contenuti risultano modificati.
- Si osservano frequenti accessi al disco fisso (la spia lampeggia).
- Il browser web (per esempio Microsoft Internet Explorer) si blocca o ha comportamenti anomali (per esempio non si riesce a chiudere la finestra del programma).

Nel 90% dei casi, questi segnali indiretti sono provocati da anomalie di funzionamento dell'hardware o del software. Malgrado questi segnali dipendano raramente da un'infezione del computer, si raccomanda di effettuare una scansione completa del computer (vedi 5.3 a pag. 65) se si dovessero manifestare.

1.5. Come comportarsi se il computer mostra segni di infezione

Se il computer ha un comportamento "sospetto":

1. Evitare il panico! Non lasciarsi prendere dal panico. È questa la regola principale da seguire in quanto può evitare la perdita di dati importanti e numerose seccature.
2. Scollegare il computer da Internet o da un'eventuale rete locale.
3. Se il sintomo riscontrato consiste nell'impossibilità di effettuare il boot dal disco fisso (il computer visualizza un messaggio d'errore all'accensione), provare ad avviare la macchina in modalità provvisoria o dal disco di boot di Windows creato durante l'installazione del sistema operativo.
4. Prima di eseguire qualsiasi operazione, effettuare una copia di backup del lavoro su un supporto esterno (floppy, CD, unità flash, ecc.).
5. Installare Kaspersky Internet Security, se non lo si è già fatto.
6. Aggiornare gli elenchi delle minacce del programma (vedi 5.7 a pag. 69). Se possibile, procurarsi gli aggiornamenti accedendo a Internet da un computer non infetto, per esempio da un amico, in un Internet point o in ufficio. È consigliabile utilizzare un computer diverso, poiché connettendosi a Internet da un computer infetto è probabile che il virus invii informazioni importanti agli hacker o si diffonda agli indirizzi presenti nella rubrica. In altre parole, se si sospetta un'infezione, la precauzione migliore è scollegarsi immediatamente da Internet. È possibile procurarsi gli aggiornamenti degli elenchi delle minacce anche su un dischetto floppy da Kaspersky Lab o dai suoi distributori e aggiornare le proprie firme dal dischetto.
7. Selezionare il livello di sicurezza raccomandato dagli esperti di Kaspersky Lab.
8. Avviare una scansione completa del computer (vedi 5.3 a pag. 65).

1.6. Prevenzione delle infezioni

Neanche le misure più affidabili e attente sono in grado di garantire una protezione assoluta dai virus e dai troiani, ma l'osservanza di queste regole riduce significativamente la probabilità di attacchi di virus e il livello di danno potenziale.

Come in medicina, una delle regole fondamentali per evitare le infezioni è la prevenzione. La profilassi del computer comporta poche regole che, se rispettate, possono ridurre in maniera considerevole la probabilità di incorrere in un virus e perdere dati.

Le regole di sicurezza fondamentali sono descritte di seguito. Osservandole è possibile evitare attacchi virulenti.

Regola 1: *Usare un software antivirus e programmi di sicurezza Internet*. Procedere come segue:

- Installare al più presto Kaspersky Internet Security.
- Aggiornare regolarmente (vedi 5.7 a pag. 69) gli elenchi delle minacce del programma. È possibile aggiornare gli elenchi più volte al giorno durante le epidemie di virus. In tali circostanze, gli elenchi delle minacce sui server di aggiornamento Kaspersky Lab vengono aggiornate istantaneamente.
- Selezionare le impostazioni di sicurezza raccomandate da Kaspersky Lab per il computer. Esse garantiscono una protezione costante dall'accensione del computer, ostacolando la penetrazione dei virus.
- Configurare le impostazioni di scansione completa raccomandate dagli esperti di Kaspersky Lab e pianificare scansioni almeno una volta la settimana. Se non si è installato Anti-Hacker, si raccomanda di provvedere in modo da proteggere il computer durante la navigazione.

Regola 2: *Usare cautela nella copia di nuovi dati sul computer*:

- Eseguire la scansione antivirus di tutte le unità di archiviazione esterne (vedi 5.5 a pag. 67) (floppy, CD, unità flash, ecc.) prima di usarle.
- Trattare i messaggi e-mail con cautela. Non aprire alcun file arrivato per posta elettronica se non si ha la certezza di esserne l'effettivo destinatario, anche se il mittente è una persona nota.
- Trattare con prudenza qualsiasi informazione ottenuta tramite Internet. Se un sito web suggerisce di installare un nuovo programma, verificare che esso abbia un certificato di sicurezza. Se si copia un file eseguibile da Internet o da una rete locale, ricordarsi di esaminarlo con Kaspersky Internet Security.
- Selezionare con prudenza i siti web da visitare. Molti siti sono infetti da script pericolosi o worm di Internet.

Regola 3: *Prestare attenzione alle informazioni fornite da Kaspersky Lab.*

Nella maggior parte dei casi, Kaspersky Lab annuncia un'epidemia con largo anticipo rispetto al periodo di massima diffusione. In tal modo le probabilità di contrarre l'infezione sono esigue, e una volta scaricati gli

aggiornamenti si disporrà di tempo a sufficienza per proteggersi dal nuovo virus.

Regola 4: *Non fidarsi delle bufale* come i programmi-scherzo (prank) e le e-mail relative a presunte infezioni.

Regola 5: *Usare lo strumento di aggiornamento di Windows* e installare regolarmente gli aggiornamenti del sistema operativo.

Regola 6: *Acquistare sempre software dotato di regolare licenza da rivenditori autorizzati.*

Regola 7: *Limitare il numero di persone che possono accedere al computer.*

Regola 8: *Contenere il rischio di conseguenze spiacevoli in caso di infezione*:

- Eseguire regolarmente una copia di backup dei dati. Se si perdono i dati, il sistema sarà in grado di ripristinarli piuttosto rapidamente se si dispone di copie di backup. Conservare in un luogo sicuro i dischetti floppy, i CD, le unità flash e altri supporti di archiviazione contenenti software e informazioni importanti.
- Creare un disco di emergenza (vedi 19.4 a pag. 287) con il quale effettuare eventualmente il boot della macchina con un sistema operativo pulito.

Regola 9: C*ontrollare regolarmente l'elenco dei programmi installati sul computer*. A tal fine, aprire **Installazione applicazioni** in **Pannello di controllo** oppure aprire la cartella **Programmi**. È possibile scoprirvi applicazioni installate all'insaputa dell'utente, per esempio durante la navigazione in Internet o l'installazione di un programma. Alcune di esse sono quasi sempre programmi potenzialmente rischiosi.

CAPITOLO 2. KASPERSKY INTERNET SECURITY 7.0

Kaspersky Internet Security 7.0 è la nuova generazione dei prodotti per la sicurezza dei dati.

La caratteristica che contraddistingue Kaspersky Internet Security 7.0 rispetto ad altri software, perfino da altri prodotti Kaspersky Lab, è l'approccio complesso alla sicurezza dei dati conservati nel computer.

2.1. Le nuove funzioni di Kaspersky Internet Security 7.0

Kaspersky Internet Security 7.0 (da questo momento denominato "Kaspersky Internet Security) offre un approccio innovativo alla sicurezza dei dati. La caratteristica principale del programma è la combinazione in un'unica soluzione delle funzioni esistenti di tutti i prodotti dell'azienda, in versione potenziata. Il programma offre protezione sia contro i virus sia contro lo spam e gli attacchi di pirateria informatica. I nuovi moduli proteggono gli utenti da minacce, phishing e rootkit non ancora noti.

In altre parole, garantisce una sicurezza globale del computer senza la necessità di installare numerosi prodotti. Solo questo è un valido motivo per installare Kaspersky Internet Security 7.0.

Tutti i canali di accesso o uscita dei dati sono protetti in maniera esauriente. Le impostazioni flessibili di ciascun componente del programma consentono di adattare in maniera ottimale Kaspersky Internet Security alle esigenze di ogni utente. È possibile inoltre impostare tutti i componenti di protezione da una singola postazione.

Esaminiamo in dettaglio le nuove funzioni di Kaspersky Internet Security 7.0.

Nuove funzionalità di protezione:

- Kaspersky Internet Security protegge il computer da programmi nocivi noti e da programmi non ancora scoperti. La difesa proattiva (vedi Capitolo 10 a pag. 132) è il vantaggio principale del programma. Esso è studiato per analizzare il comportamento delle applicazioni installate sul computer, monitorare le modifiche al registro di sistema, individuare le macro e combattere le minacce nascoste. Il componente si basa su un analizzatore euristico in grado di individuare vari tipi di programmi

nocivi. Così facendo, compila una cronologia delle attività nocive grazie alla quale è possibile retrocedere e ripristinare l'ultima versione sicuramente funzionante del sistema prima dell'attività nociva.

- Il programma protegge da rootkit e dialer, blocca i banner pubblicitari, i popup e gli script nocivi scaricati dalle pagine web, individua i siti di phishing e protegge gli utenti dalla trasmissione non autorizzata di dati riservati (password per connessioni Internet, e-mail o server ftp).

- La tecnologia di File Anti-virus è stata potenziata per ridurre il carico sul processore centrare e i sottosistemi del disco e aumentare la velocità di scansione dei file utilizzando le tecnologie iCheck e iSwift. In questo modo, il programma evita di analizzare i file due volte.

- Il processo di scansione si svolge adesso in modalità secondaria mentre l'utente continua a usare il computer. Una scansione può comportare un dispendio considerevole di tempo e di risorse di sistema, ma non è necessario che l'utente interrompa la propria attività con il computer. Se un'operazione richiede maggiori risorse di sistema, la scansione si interrompe fino a quando l'operazione sarà conclusa. La scansione riprende quindi dal punto in cui si era interrotta.

- Per le aree critiche del computer e per gli oggetti di avvio che potrebbero causare seri problemi se infettate e per rilevare i rootkit utilizzati per nascondere il software nocivo sul computer sono previste attività individuali. Queste attività possono essere configurate in modo da eseguirsi automaticamente ad ogni avvio del sistema.

- La protezione della posta elettronica contro i programmi nocivi e lo spam è stata considerevolmente migliorata. Il programma esegue la scansione antivirus e antispam delle e-mail inviate con i seguenti protocolli:

  - IMAP, SMTP, POP3, indipendentemente dal client di posta utilizzato.

  - NNTP (solo scansione antivirus), indipendentemente dal client di posta utilizzato.

  - MAPI, HTTP (con i plug-in per MS Outlook e The Bat!).

- Sono disponibili plug-in specifici per i client di posta più comuni come Outlook, Microsoft Outlook Express e The Bat!, che consentono di configurare direttamente dal client la protezione antivirus e antispam della posta.

- La funzionalità Anti-Spam si espande man mano che la casella della posta in entrata si riempie, registrando le azioni dell'utente nei confronti della posta e garantendo così la massima flessibilità di configurazione. L'apprendimento progressivo da parte del programma si basa

sull'algoritmo di iBayes. È possibile compilare liste bianche e liste nere di indirizzi di mittenti e di espressioni ricorrenti nei messaggi identificati come spam.

La funzione Anti-spam fa uso di un database di phishing in grado di escludere tutte le e-mail studiate per procurare informazioni confidenziali di natura finanziaria.

- Il programma filtra la posta in arrivo e quella in uscita, individua e blocca le minacce da attacchi di rete comuni e consente di utilizzare Internet in modalità invisibile.
- La funzione di notifica dell'utente (vedi 19.9.1 a pag. 301) è stata ampliata includendo determinati eventi che si verificano durante il funzionamento del programma. È possibile scegliere per ciascun evento uno dei seguenti metodi di notifica: e-mail, segnalazione acustica, messaggi a comparsa.
- È stata aggiunta la funzionalità di scansione del traffico inviato sul protocollo SSL.
- Il programma è dotato di funzionalità di autodifesa: Protezione dall'utilizzo remoto non autorizzato dei servizi di Kaspersky Internet Security, e impostazioni del programma protette da password. Queste funzioni impediscono ai programmi nocivi, agli hacker e agli utenti non autorizzati di disabilitare la protezione.
- È stata aggiunta la possibilità di creare un disco di emergenza. Grazie a questo disco, è possibile riavviare il sistema operative dopo l'attacco di un virus e sottoporlo a scansione per rilevare la presenza di oggetti nocivi.
- Un nuovo componente di Kaspersky Internet Security, Controllo contenuti, consente agli utenti di monitorare l'accesso a Internet del computer. Questa funzione permette o blocca l'accesso degli utenti a determinate risorse Internet. Inoltre, questo componente limita anche il tempo di permanenza ondine.
- È stato aggiunto il componente News Agent. Si tratta di un modulo concepito per la notifica in tempo reale di notizie da parte di Kaspersky Lab.
- È stato potenziato il supporto per il protocollo IP, Versione 6 (IPv6).

Nuove funzioni dell'interfaccia

- La nuova interfaccia di Kaspersky Internet Security agevola l'uso delle funzioni del programma. È possibile anche modificare l'aspetto del programma creando e utilizzando una grafica e uno schema cromatico personalizzati.

- Il programma offre regolarmente suggerimenti durante l'uso: Kaspersky Internet Security visualizza messaggi informativi sul livello di protezione, accompagna il proprio funzionamento con suggerimenti e consigli e offre un'esauriente guida.

Nuove funzioni di aggiornamento del programma

- Questa versione del programma introduce una nuova e più potente procedura di aggiornamento: Kaspersky Internet Security controlla automaticamente le origini di aggiornamento per verificare la disponibilità dei pacchetti di aggiornamento. Non appena li rileva, li scarica e li installa sul computer.
- Il programma scarica solo gli aggiornamenti non ancora installati. In tal modo il traffico verso i server di aggiornamento risulta ridotto fino a 10 volte.
- Gli aggiornamenti sono scaricati dall'origine più efficiente.
- Oggi è possibile scegliere di non utilizzare un server proxy se gli aggiornamenti del programma vengono scaricati da un'origine locale. Ciò riduce considerevolmente il carico sul server proxy.
- Il programma è dotato di una funzione di ripristino dello stato precedente, che consente di ripristinare l'ultima versione sicuramente funzionante delle firme se, per esempio, le firme installate risultano danneggiate o si è verificato un errore durante la copia.
- È stata aggiunta una funzione per distribuire gli aggiornamenti in una cartella locale, al quale possono accedere gli altri computer sulla rete. In questo modo si risparmia ampiezza di banda.

2.2. I componenti di protezione di Kaspersky Internet Security

La protezione di Kaspersky Internet Security è stata studiata tenendo conto delle provenienze delle minacce. In altre parole, ogni tipo di minaccia è gestito da un componente distinto del programma, monitorato e affrontato con le misure necessarie a impedirne gli effetti nocivi sui dati dell'utente. Questa struttura rende flessibile la Security Suite, offrendo facili opzioni di configurazione per tutti i componenti in modo da soddisfare le esigenze di utenti specifici o aziende nella loro globalità.

Kaspersky Internet Security presenta:

- Componenti di protezione in tempo reale (vedi 2.2.1 a pag. 26) per una difesa globale su tutti i canali di trasmissione e scambio dati del computer.
- Attività di scansione antivirus (vedi 2.2.2 a pag. 28) che esaminano il computer o singoli file, cartelle, dischi o aree alla ricerca di virus.
- Aggiornamenti (vedi 2.2.3 a pag. 29) per garantire l'attualità dei moduli dell'applicazione e degli aggiornamenti dei database utilizzati per scansionare software nocivo, attacchi degli hacker e spam.

2.2.1. Componenti di protezione in tempo reale

I componenti di protezione garantiscono la sicurezza del computer in tempo reale:

File Anti-Virus

Un file system può contenere virus e altri programmi pericolosi. I programmi nocivi possono restare nel file system per anni dopo esservi stati introdotti attraverso un dischetto floppy o navigando in Internet, senza mostrare la propria presenza. Ma è sufficiente aprire il file infetto o, per esempio, provare a copiarlo su un disco, per attivare immediatamente il file.

File Antivirus è il componente che monitora il file system del computer. Esso esamina tutti i file che possono essere aperti, eseguiti o salvati sul computer e su tutte le unità disco collegate. Kaspersky Internet Security intercetta ogni file che viene aperto e lo esamina per escludere la presenza di virus noti. Il file esaminato potrà essere utilizzato solo se non infetto o se successivamente trattato mediante File Anti-Virus. Se per qualsiasi motivo non fosse possibile riparare un file infetto, esso viene eliminato dopo averne salvata una copia nella cartella Backup (vedi 19.2 a pag. 267), o trasferito in Quarantena (vedi 19.1 a pag. 263).

Mail Anti-Virus

La posta elettronica è molto utilizzata dagli hacker per diffondere programmi nocivi e rappresenta uno dei canali più diffusi per la diffusione di worm. Per questo è estremamente importante monitorare tutta la posta.

Mail Anti-Virus è il componente che esamina tutti i messaggi e-mail in entrata e in uscita dal computer, in cerca di programmi nocivi. Il programma consente al destinatario di aprire il messaggio solo se privo di oggetti pericolosi.

Web Anti-Virus

Ogni volta che si apre un sito web si corre il rischio di restare infettati dai virus presenti negli script eseguiti sui siti web, e di scaricare oggetti pericolosi sul proprio computer.

Web Anti-Virus è pensato specificamente per prevenire tali evenienze. Questo componente intercetta e blocca gli script dei siti web potenzialmente pericolosi, monitorando accuratamente tutto il traffico HTTP.

Difesa proattiva

Ogni giorno compaiono nuovi programmi nocivi in quantità crescente. Essi diventano sempre più complessi combinando più tipi di minaccia, e i metodi utilizzati per diffondersi sono sempre più difficili da scoprire.

Per individuare un nuovo programma nocivo prima che abbia il tempo di provocare danni, Kaspersky Lab ha sviluppato uno speciale componente dal nome *Difesa proattiva*. Esso è progettato per monitorare e analizzare il comportamento di tutti i programmi installati sul computer. Kaspersky Internet Security prende una decisione in base alle azioni eseguite da un'applicazione: il programma è pericoloso? Difesa proattiva protegge il computer sia dai virus noti sia da quelli non ancora scoperti.

Controllo privacy

Varie truffe online recentemente sono sempre più diffuse (phishing, dialer a composizione automatica, sottrazione di dati confidenziali come dati di accesso e password). Queste azioni possono causare seri danni finanziari.

Controllo privacy tiene traccia di questi tentativi di truffa sul computer e li blocca. Per esempio, questo componente blocca i programmi che tentano di eseguire la composizione di numeri telefonici non autorizzati, analizzano le pagine web per tentativi di phishing, intercettano l'accesso non autorizzato e i download di dati personali.

Firewall

Gli hacker sfruttano le potenziali falle della rete per invadere il computer dell'utente, siano esse porte aperte, trasmissioni di dati tra computer, ecc.

Il componente *Firewall* protegge il computer durante la navigazione su Internet e altre reti. Monitora le connessioni in entrata e in uscita, e analizza le porte e i pacchetti di dati.

Inoltre, Firewall blocca la pubblicità indesiderata (banner pubblicitari e finestre pop-up), riducendo così il traffico scaricato da Internet e facendo risparmiare tempo all'utente.

Anti-Spam

Benché non sia una minaccia diretta al computer, lo spam aumenta il carico sui server di posta, riempie le caselle di posta e fa perdere tempo, rappresentando così un costo in termini lavorativi.

Il componente *Anti-Spam* si installa sul client di posta elettronica dei computer e analizza tutti i messaggi in entrata per verificare la presenza di spam. Il componente marca tutte le e-mail contenenti spam con una speciale intestazione. Anti-Spam può essere configurato per elaborare lo spam a piacimento dell'utente (eliminazione automatica, trasferimento in una cartella speciale, ecc.).

Controllo contenuti

Una delle caratteristiche di Internet è la mancanza di censura: pertanto, molti siti web contengono informazioni illegali o indesiderate, o informazioni dirette a un pubblico adulto. Sempre più siti contengono contenuti di razzismo, pornografia, violenza, uso di armi e di sostanze stupefacenti. Inoltre, spesso questi siti contengono numerosi programmi nocivi che si eseguono non appena vengono visitati.

La limitazione dell'accesso a questi siti web, in particolare per i minori, è una funzione chiave dei nuovi software di protezione dei dati.

Controllo contenuti è un componente messo a punto per controllare l'accesso dell'utente a determinati siti su Internet. Si può trattare di siti con contenuto opinabile o altri siti che l'utente seleziona nelle impostazioni di Kaspersky Internet Security. Il controllo può essere applicato non solo sul contenuto delle risorse, ma anche sul tempo trascorso online. L'accesso a Internet può essere consentito in certi orari e può essere posto un limite al tempo totale speso online entro un periodo di 24 ore.

2.2.2. Attività di scansione antivirus

Oltre a monitorare costantemente i potenziali accessi di programmi nocivi, è estremamente importante eseguire periodicamente la scansione antivirus del computer. Ciò è necessario al fine di escludere la possibilità di diffondere programmi nocivi non ancora rilevati dai componenti di sicurezza a causa della protezione impostata su un livello basso o per altri motivi.

Kaspersky Internet Security offre tre attività di scansione antivirus:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer, fra cui: memoria di sistema, programmi caricati all'avvio, settori di boot del disco fisso, directory di sistema *Windows* e *system32*. L'obiettivo di questa

attività è individuare rapidamente i virus attivi nel sistema senza eseguire una scansione completa del computer.

Risorse del computer

La scansione antivirus viene effettuata sull'intero computer, con un'analisi approfondita di tutte le unità disco, memoria e file.

Oggetti di avvio

La scansione antivirus viene effettuata su tutti i programmi caricati automaticamente all'avvio, sulla RAM e sui settori di boot dei dischi fissi.

Scansione Rootkit

Esegue la scansione per rilevare rootkit che nascondono programmi nocivi nel sistema operativo. Queste utility inserite nel sistema, nascondono la propria presenza e quella di processi, cartelle, chiavi di registro di qualsiasi programma nocivo descritto nella configurazione del rootkit.

È possibile inoltre creare altre attività di ricerca dei virus e pianificarne l'esecuzione. Per esempio, è possibile creare un'attività di scansione per i database della posta da eseguire una volta la settimana, o un'attività di scansione antivirus della cartella **Documenti**.

2.2.3. Update

Per essere sempre in guardia contro gli attacchi degli hacker ed essere pronti ad eliminare un virus o qualche altro programma pericoloso, Kaspersky Internet Security necessita di un supporto in tempo reale. La funzione *Aggiornamento* è messa a punto per svolgere esattamente questa funzione. È responsabile dell'aggiornamento dei database e dei moduli dell'applicazione utilizzati da Kaspersky Internet Security.

La funzione di distribuzione degli aggiornamenti consente di salvare i database e I moduli del programma recuperati dai server di Kaspersky Lab in una cartella locale e consentire l'accesso a tale cartella agli altri computer sulla rete per ridurre il traffico Internet.

2.2.4. Strumenti del programma

Kaspersky Internet Security offre una serie di strumenti di supporto progettati per fornire assistenza software in tempo reale, espandendo le funzionalità del programma e assistendo l'utente durante la procedura.

Report e file dati

Quando è in esecuzione, l'applicazione genera un report su ogni componente di protezione in tempo reale, operazione di scansione e aggiornamento dei database. Contiene informazioni sui risultati e le operazioni eseguite. I dettagli su tutti i componenti di Kaspersky Internet Security sono disponibili attraverso la funzione *Rapporto*. In caso di problemi, questi report possono essere inoltrati a Kaspersky Lab affinché i nostri esperti possano esaminare più attentamente la situazione e fornire assistenza al più presto.

Tutti gli oggetti sospetti vengono posti da Kaspersky Internet Security in una speciale area nota come *Quarantena* dove vengono memorizzati in un formato codificato per proteggere il computer dalle infezioni. Questi oggetti possono essere sottoposti a scansione anti-virus, ripristinati nella posizione originale o eliminati. Gli oggetti possono essere trasferiti in quarantena manualmente. Tutti gli oggetti rilevati dalla scansione che devono essere disinfettati vengono automaticamente ripristinati nella posizione originale.

La cartella Backup contiene le copie disinfettate o eliminate dall'applicazione. Queste copie vengono create in caso sia necessario ripristinare gli oggetti o ricostruire il corso della loro infezione. Anche le copie di backup sono memorizzate in formato codificato per proteggere il computer da infezioni. Un oggetto di cui è stato creato il backup può essere ripristinato nella posizione originale oppure eliminato.

Attivazione

Al momento dell'acquisto di Kaspersky Internet Security, l'utente stipula un contratto di licenza con Kaspersky Lab che regolamenta l'uso dell'appliaczione oltre all'accesso ai database di aggiornamento dell'applicazione e al Supporto tecnico per un determinato periodo di tempo. Le condizioni d'uso e altre informazioni necessarie per la completa funzionalità del programma sono fornite nel file della chiave.

Dalla funzione *Attivazione*, si accede a informazioni dettagliate sulla chiave utilizzata o sull'acquisto di una nuova chiave.

Supporto

Tutti gli utenti registrati di Kaspersky Internet Security possono avvalersi del nostro Servizio di assistenza tecnica. Per informazioni su come ottenere tale assistenza, usare la funzione *Supporto*.

Seguendo questi link si arriva al forum di Kaspersky Lab, oppure inviare un feedback o riferire un errore al Supporto Tecnico compilando lo speciale modulo online.

Vi troverete un elenco delle domande più frequenti che potrebbero essere sufficienti a risolvere il problema. Ma è possibile anche accedere all'Assistenza web, ai servizi di Assistenza personalizzata e, naturalmente, i

nostri esperti saranno disponibili telefonicamente o per e-mail per risolvere qualsiasi problema legato all'uso di Kaspersky Internet Security.

2.3. Requisiti di sistema hardware e software

Per garantire il corretto funzionamento di Kaspersky Internet Security 7.0, il computer deve possedere i seguenti requisiti minimi:

Requisiti di carattere generale:

- 50 MB di spazio disponibile sul disco fisso.
- CD-ROM (per installare Kaspersky Internet Security 7.0 dal CD di installazione).
- Microsoft Internet Explorer 5.5 o superiore (per aggiornare gli elenchi delle minacce e i moduli del programma attraverso Internet).
- Microsoft Windows Installer 2.0.

Microsoft Windows 2000 Professional (Service Pack 2 o superiore), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 2 o superiore), Microsoft Windows XP Professional x64 Edition:

- Processore Intel Pentium 300 MHz o superiore (o compatibile).
- 128 MB di RAM.

Microsoft Windows Vista, Microsoft Windows Vista x64:

- Intel Pentium 800 MHz a 32 bit (x86)/ 64-bit (x64) o superiore (o compatibile)
- 512 MB di RAM

2.4. Pacchetti software

Kaspersky Internet Security può essere acquistato presso i nostri rivenditori, nella versione in scatola, oppure via Internet (per esempio su www.kaspersky.it, nella sezione **eStore**).

La versione in scatola include:

- Una busta sigillata con CD di installazione contenente i file del programma e la documentazione in formato PDF.

- Un manuale dell'utente in versione cartacea (se questa voce è stata inclusa nell'ordine) o un manuale d'uso del prodotto.
- Il codice di attivazione del programma, applicato sulla busta del CD di installazione.
- Il contratto di licenza con l'utente finale (EULA).

Prima di rompere il sigillo della busta contenente il CD di installazione, leggere attentamente l'EULA.

Chi acquista Kaspersky Internet Security attraverso Internet, copierà il prodotto dal sito web di Kaspersky Lab (**Downloads → Product Downloads**). Il manuale d'uso del prodotto può essere scaricato nella sezione **Downloads → Documentation**.

A pagamento avvenuto, l'utente riceverà per e-mail il codice di attivazione.

Il Contratto di licenza con l'utente finale è un accordo con valore legale fra l'utente finale e Kaspersky Lab, volto a regolamentare le condizioni di utilizzo del prodotto acquistato.

Leggere attentamente l'EULA.

Se non si accettano i termini del Contratto di licenza, è possibile restituire il prodotto completo di scatola al distributore presso cui è stato effettuato l'acquisto, e ottenere il rimborso completo dell'importo pagato. Ciò è possibile a condizione che la busta contenente il CD di installazione sia ancora sigillata.

L'apertura della busta sigillata del CD di installazione comporta l'accettazione dei termini e delle condizioni del Contratto di licenza da parte dell'acquirente.

2.5. Assistenza per gli utenti registrati

Kaspersky Lab offre ai propri utenti registrati una serie di servizi volti ad ottimizzare l'efficacia di Kaspersky Internet Security.

Dopo l'attivazione del programma si diventa automaticamente utenti registrati e si ha diritto ai seguenti servizi fino alla scadenza della licenza:

- Aggiornamenti a cadenza oraria dei database dell'applicazione e nuove versioni del programma, a titolo gratuito.
- Consulenza telefonica e via e-mail su problematiche relative all'installazione, alla configurazione e al funzionamento del programma.

- Comunicazioni sui nuovi prodotti di Kaspersky Lab e sui nuovi virus (questo servizio è riservato agli utenti iscritti alla newsletter di Kaspersky Lab sul sito web del Supporto Tecnico http://support.kaspersky.com/subscribe/).

Kaspersky Lab non fornisce assistenza tecnica relativa all'uso e al funzionamento del sistema operativo o di qualsiasi altro prodotto di altri fabbricanti.

CAPITOLO 3. INSTALLAZIONE DI KASPERSKY INTERNET SECURITY 7.0

Kaspersky Internet Security 7.0 può essere installato su un host in vari modi:

- in modo interattivo, utilizzando la procedura guidata di installazione (vedi 3.1 a pag. 34) questa modalità richiede un'immissione da parte dell'utente affinché l'installazione proceda;
- in modo non interattivo; questo tipo di installazione è eseguito dalla riga di comando e non richiede alcuna immissione da parte dell'utente (vedere 3.3 a pag. 51).

Attenzione!

Prima di avviare l'installazione di Kaspersky Internet Security raccomandiamo di chiudere tutte le altre applicazioni.

3.1. Installazione utilizzando la procedura guidata

Nota:

La procedura di installazione per mezzo di un pacchetto scaricato da Internet è uguale a quella per mezzo del CD.

Per installare Kaspersky Internet Security sul computer, avviare il file di installazione sul CD (file con estensione **.exe*).

Tale file cercherà di localizzare il pacchetto di installazione dell'applicazione (file con estensione **.msi*) e, in caso di esito positivo, all'utente viene chiesto di verificare la presenza di aggiornamenti di Kaspersky Internet Security sui server Kaspersky Lab. Se non viene trovato alcun pacchetto di installazione, il prodotto dovrà essere scaricato. In seguito al download, inizia il processo di installazione. Se l'utente sceglie di non procedere al download, l'installazione continuerà normalmente.

Si apre una procedura di installazione guidata del programma. Ogni finestra contiene dei pulsanti che consentono di completare il processo. Ecco una breve descrizione delle loro funzioni:

- **Avanti** – conferma un'azione e apre la fase successiva dell'installazione.
- **Indietro** – riporta alla fase precedente dell'installazione.
- **Cancella** – annulla l'installazione del prodotto.
- **Fine** – completa la procedura di installazione del programma.

Osserviamo in dettaglio le fasi della procedura di installazione.

Passaggio 1. Verificare i requisiti di sistema per l'installazione di Kaspersky Internet Security

Prima di installare il programma sul computer, l'installer controlla che il sistema operativo e i service pack necessari per l'installazione di Kaspersky Internet Security. L'applicazione controlla inoltre che il computer disponga di altri programmi necessari e che l'utente possieda diritti sufficienti per l'installazione di software.

In assenza di uno qualsiasi dei requisiti necessari, il programma visualizza un messaggio informando l'utente dell'impossibilità di completare l'installazione. Prima di installare Kaspersky Internet Security si raccomanda di installare i service pack necessari attraverso **Windows Update** ed eventuali altri programmi.

Passaggio 2. Finestra di avvio dell'installazione

Se il sistema soddisfa tutti i requisiti necessari, non appena si esegue il file di installazione si apre una finestra che avvisa dell'inizio dell'installazione di Kaspersky Internet Security.

Per continuare l'installazione fare clic su **Avanti**. Per annullare l'installazione fare clic su **Annulla**.

Passaggio 3. Visualizzazione del Contratto di licenza con l'utente finale

La finestra di dialogo successiva contiene un Contratto di licenza tra l'acquirente e Kaspersky Lab. Leggere attentamente il contratto e, se si approvano le condizioni, fare clic su **Accetto i termini dell'accordo di licenza,** quindi premere il pulsante **Avanti**. L'installazione prosegue.

Passaggio 4. Selezione del tipo di installazione

In questo passaggio, l'utente deve selezionare un tipo di installazione:

Installazione Express. Selezionando questa opzione, Kaspersky Internet Security viene installato unicamente secondo le impostazioni predefinite, come consigliato dagli esperti di Kaspersky Lab. Al termine dell'installazione, sarà avviata una procedura guidata di attivazione (vedere 3.2.2 a pag. 40).

Installazione Personalizzata. Questa opzione consente di selezionare i componenti dell'applicazione da installare, la cartella di installazione, e di attivare il prodotto e configurare l'installazione utilizzando una speciale procedura guidata (vedi 3.2 a pag. 39).

Nel primo caso, l'installazione non sarà interattiva, cioé i passaggi successivi descritti nella presente sezione saranno ignorati. Nel secondo caso, l'utente sarà invitato a immettere o confermare determinati dati.

Passaggio 5. Selezione di una cartella di installazione

La fase successiva dell'installazione di Kaspersky Internet Security serve per stabilire la posizione in cui installare il programma sul computer. Il percorso predefinito è:

- Per i sistemi a 32 bit: **<Drive> → Programmi → Kaspersky Lab → Kaspersky Internet Security 7.0**
- Per i sistemi a 64 bit: **<Drive> → Programmi (x86) → Kaspersky Lab → Kaspersky Internet Security 7.0**

Per specificare una cartella diversa, fare clic sul pulsante **Sfoglia** e selezionare la nuova cartella nella finestra di selezione che si apre, oppure digitare direttamente il percorso nel campo apposito.

Attenzione!

Ricordare che se si desidera digitare manualmente il percorso completo della cartella di installazione esso non deve superare i 200 caratteri né contenere caratteri speciali.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 6. Selezione dei componenti da installare

Nota:

Questa fase si presenta solo se è stata selezionata l'installazione **Personalizzata**.

Se è stata selezionata l'installazione personalizzata, è necessario selezionare i componenti di Kaspersky Internet Security che si desidera installare. Le selezioni predefinite includono tutte le funzioni antivirus e i componenti di scansione antivirus. Anti-Hacker, Anti-Spam e Anti-Spy non vengono installati.

Per selezionare i componenti desiderati, fare clic con il pulsante destro del mouse sull'icona a fianco del nome di un componente e selezionare **Utilizzo disco** dal menu contestuale. Ulteriori informazioni sul tipo di protezione offerto da un determinato componente e sulla quantità di spazio su disco necessario per l'installazione sono disponibili nella parte inferiore della finestra del programma di installazione.

Se non si desidera installare un componente, selezionare **Questa funzionalità non sarà più disponibile** dal menu contestuale. Ricordare che, scegliendo di non installare un componente, ci si priva di un elemento di protezione da una vasta gamma di programmi pericolosi.

Dopo aver selezionato i componenti da installare, fare clic su **Avanti**. Per tornare all'elenco dei programmi predefiniti da installare, fare clic su **Reimposta**.

Passaggio 7. Disabilitazione della firewall di Microsoft Windows

Questa fase viene visualizzata solo se si sta installando il componente Firewall di Kaspersky Internet Security su un computer con la firewall incorporata di *Microsoft Windows* abilitata.

In questa fase, Kaspersky Internet Security chiede se si desidera disabilitare la firewall di Microsoft Windows poiché il componente Firewall, incluso in Kaspersky Internet Security offre una protezione firewall completa.

Se si desidera utilizzare Firewall come principale protezione di rete, fare clic su **Avanti**. Il firewall di Microsoft Windows viene disabilitato automaticamente.

Se invece si desidera mantenere e utilizzare il firewall di Windows, selezionare **Mantieni firewall Windows abilitata**. Se si seleziona questa opzione, il componente Firewall di Kaspersky Internet Security sarà installato ma disabilitato per evitare conflitti tra programmi.

Passaggio 8. Utilizzo delle impostazioni di installazione salvate precedentemente

In questo passaggio, l'utente deve specificare se intende importare le impostazioni di protezione, inclusi i database di Anti-Spam salvati sul computer nel momento in cui è stata rimossa una versione precedente di Kaspersky Internet Security.

Alla suddetta funzionalità si accede nel seguente modo.

Se sul computer era installata una versione precedente di Kaspersky Internet Security e i database dell'applicazione sono stati salvati, questi possono essere importati nella versione in fase di installazione. Selezionare l'opzione **Database applicazione**. I database incorporati nell'applicazione non saranno copiati sul computer.

Per utilizzare le impostazioni di protezione configurate per una versione precedente e salvate sul computer, selezionare **Impostazioni runtime.**

Si consiglia inoltre di utilizzare i database di Anti-Spam, a condizione che siano stati salvati quando la versione precedente è stata rimossa. Questo consentirà di saltare l'addestramento di Anti-Spam. Per utilizzare i database esistenti, selezionare **Database Anti-Spam**.

Passaggio 9. Ricerca di altri programmi antivirus

In questa fase, l'installer cerca altri programmi antivirus presenti sul computer, compresi altri prodotti Kaspersky Lab, che potrebbero provocare problemi di compatibilità con Kaspersky Internet Security.

Se l'installer individua questo tipo di programmi, ne visualizza un elenco sul video. Il programma chiede se si desidera disinstallarli prima di proseguire l'installazione.

È possibile selezionare la disinstallazione manuale o automatica nell'elenco delle applicazioni antivirus individuate.

Se l'elenco dei programmi antivirus contiene Kaspersky Internet Security 6.0, si raccomanda di salvare le chiavi di licenza utilizzate prima di procedere a una disinstallazione manuale, in quanto possono essere utilizzate anche per Kaspersky Internet Security 7.0. Si raccomanda inoltre di salvare gli oggetti della Quarantena e del Backup. Essi saranno trasferiti automaticamente nelle aree Quarantena e Backup di Kaspersky Internet Security da dove è possibile continuare a usarli.

Qualora Kaspersky Internet Security 6.0 venga disinstallato automaticamente, le informazioni di attivazione saranno salvate dal software e saranno soprascritte durante l'installazione della versione 7.0.

Attenzione!

Kaspersky Internet Security 7.0 supporta i file chiave della Versione 6.0 e della Versione 7.0. Le chiavi utilizzate per la Versione 5.0 non sono supportate.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 10. Completamento dell'installazione

In questa fase, il programma chiede di completare l'installazione del programma sul computer.

Non consigliamo di deselezionare **Abilita Auto-Difesa prima dell'installazione** quando si avvia l'installazione di Kaspersky Internet Security. Abilitando i moduli di protezione, è possibile correttamente retrocedere con l'installazione se si commettono errori durante l'installazione del programma. Se state reinstallando il programma consigliamo di deselezionare questa casella di spunta.

Se l'applicazione viene installata da remoto via **Windows Remote Desktop** consigliamo di deselezionare **Abilita Auto-Difesa prima dell'installazione**. In caso contrario la procedura di installazione potrebbe non completarsi o completarsi in modo errato.

Per continuare l'installazione fare clic su **Avanti**.

Attenzione!

Le correnti connessioni di rete sono cadute durante l'installazione di componenti di Kaspersky Anti-Virus che intercettano il traffico di rete. La maggior parte delle connessioni di rete vengono ristabilite dopo un dato intervallo di tempo.

Passaggio 11. Completamento della procedura di installazione

La finestra **Installazione completata** contiene informazioni su come portare a termine la procedura di installazione di Kaspersky Internet Security.

Per completare correttamente l'installazione è necessario riavviare il computer, seguendo il suggerimento del messaggio visualizzato sullo schermo. Dopo il riavvio del sistema, si apre automaticamente la finestra della procedura di ipostazione guidata di Kaspersky Internet Security.

Se non è richiesto il riavvio del sistema, fare clic su **Avanti** per passare alla procedura di impostazione guidata.

3.2. Impostazione guidata

La procedura di impostazione guidata di Kaspersky Internet Security 7.0 inizia al termine dell'installazione del programma e serve per agevolare la configurazione delle impostazioni iniziali del programma in base alle caratteristiche e agli usi del computer.

L'interfaccia della procedura guidata è analoga a quelle delle procedure guidate standard di Windows e consiste di una serie di passaggi tra i quali è possibile spostarsi per mezzo dei pulsanti **Indietro** e **Avanti**, o che è possibile portare a termine facendo clic sul pulsante **Fine.** Il pulsante **Annulla** serve per interrompere in qualsiasi momento la procedura.

È possibile omettere questa fase iniziale di impostazione durante l'installazione del programma chiudendo la finestra della procedura guidata. Sarà possibile eseguirla di nuovo in seguito dall'interfaccia del programma se si ripristinano le impostazioni predefinite di Kaspersky Internet Security (vedi 19.9.4 a pag. 307).

3.2.1. Uso di oggetti salvati con la versione 5.0

Questa finestra della procedura guidata si apre quando si installa l'applicazione su Kaspersky Anti-Virus 5.0. L'utente dovrà selezionare i dati che desidera importare dalla versione 5.0 alla 7.0, compresi i file conservati nelle cartelle Quarantena e Backup e le impostazioni di protezione.

Per utilizzare questi oggetti nella versione 7.0, selezionare le caselle appropriate.

3.2.2. Attivazione del programma

Prima di attivare il programma accertarsi che la regolazione della data del sistema corrisponda alla data ed ora attuale.

È possibile attivare il programma installando una chiave di licenza che Kaspersky Internet Security utilizzerà per verificare il contratto di licenza e determinarne la data di scadenza.

La chiave di licenza contiene informazioni di sistema necessarie per il corretto funzionamento del prodotto, oltre a informazioni relative a:

- Assistenza (chi la fornisce e come ottenerla).
- Nome, numero e data di scadenza della licenza.

3.2.2.1. Selezione di un metodo di attivazione del programma

A seconda che si disponga di una chiave di licenza per Kaspersky Internet Security o sia necessario scaricarne una dal server Kaspersky Lab, è possibile scegliere varie opzioni di attivazione del programma:

- **Attiva mediante codice di attivazione**. Selezionare questa opzione di attivazione se è stata acquistata la versione completa del programma con codice di attivazione in dotazione. Questo codice consente di ottenere una chiave di licenza che garantisce l'accesso completo a tutte le funzionalità del programma fino alla scadenza della licenza.
- **Attiva versione di valutazione (30 giorni)).** Selezionare questa opzione di attivazione se si desidera installare la versione di prova del programma prima di decidere se acquistare la versione commerciale. In questo caso l'utente riceverà una chiave di licenza gratuita della durata di 30 giorni.
- **Applica chiave di licenza**. Selezionare questa opzione di attivazione se già si dispone di un file chiave di licenza per Kaspersky Internet Security 7.0.
- **Attiva successivamente**. Selezionando questa opzione si omette la fase di attivazione. Kaspersky Internet Security 7.0 viene installato sul computer e si potrà accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (è possibile aggiornare gli elenchi delle minacce solo dopo l'installazione del programma).

Attenzione!

È necessario disporre di una connessione Internet per le prime due opzioni di attivazione. Se al momento dell'installazione non si dispone di una connessione Internet, si può procedere all'attivazione in un secondo momento (vedi Capitolo 18 a pag. 260) utilizzando l'interfaccia dell'applicazione o collegandosi ad Internet da un altro computer, e ottenere una chiave utilizzando un codice di attivazione fornito registrandosi sul sito web del supporto tecnico di Kaspersky Lab.

3.2.2.2. Inserimento del codice di attivazione

Per attivare il programma è necessario inserire il codice di attivazione. Acquistando l'applicazione attraverso Internet il codice di attivazione è inviato via e-mail. Nel caso di acquisto da un rivenditore il codice di attivazione è riportato sul disco di installazione.

Il codice di attivazione è una sequenza di numeri, separati da trattini in quattro gruppi di cinque simboli senza spazi. Ad esempio 11AA1-11AAA-1AA11-1A111. Il codice di attivazione deve essere digitato inserendo caratteri Latini.

In caso l'utente sia già registrato sul sito web del servizio di supporto tecnico e disponga di un numero cliente e di una password, abilitare la casella di selezione **Ho già una ID cliente** e immettere i dati nella parte inferiore della finestra.

Se non ci si è ancora registrati, premere il pulsante **Avanti** lasciando la casella deselezionata. Se è già stata eseguita la procedura di registrazione cliente Kaspersky Lab e si dispone di queste informazioni, immettere il proprio numero cliente e la password nella parte inferiore della finestra. Lasciare tali campi in bianco se la registrazione non è ancora avvenuta. La procedura guidata di registrazione chiederà le informazioni di recapito ed eseguirà la registrazione nel passaggio successivo. Al termine della registrazione, l'utente riceverà un numero cliente e una password, necessari per usufruire del supporto tecnico. Quando ci si registra utilizzando la procedura guidata di attivazione, il numero cliente può essere visualizzato nella sezione Supporto della finestra principale dell'applicazione (vedi 19.10 a pag. 308).

3.2.2.3. Registrazione dell'utente

Questo passaggio della procedura guidata di attivazione chiede di fornire le vostre coordinate: indirizzo e-mail, Paese e città di residenza. Queste informazioni sono necessarie al Supporto Tecnico di Kaspersky Lab per identificarvi correttamente come utente registrato.

Dopo questo inserimento l'informazione viene inviata dalla procedura guidata di attivazione ad un server e vi verrà assegnato un ID cliente ed una password per la cabina personale riservata sul sito web del supporto tecnico. L'informazione circa l'ID cliente è disponibile in **Supporto** (vedi 19.10 a pag. 308) nella finestra principale dell'applicazione.

3.2.2.4. Ottenimento di una chiave di licenza

La procedura guidata stabilisce il collegamento con i server Kaspersky Lab ai quali invia i dati di registrazione (il codice di attivazione e le informazioni personali), che saranno quindi esaminati sul server stesso.

Se il codice di attivazione risulta valido, l'applicazione riceve un file con la chiave di licenza. Se si installa la versione demo del programma (con un periodo di prova di 30 giorni), la procedura guidata riceve un file chiave di prova senza codice di attivazione.

Esso viene installato automaticamente e, al termine della procedura, si apre una finestra di completamento dell'attivazione contenente informazioni dettagliate sulla licenza.

Nota

Quando viene selezionato questo metodo di attivazione, l'applicazione non scarica un file fisico con estensione *.key da un server, ma ricava determinati dati presenti sul registro del sistema operativo e nel the file system.

La registrazione dell'utente sul sito web di Kaspersky Lab è necessaria per ottenere una chiave di attivazione effettiva.

Se il codice di attivazione non risulta valido, si apre sullo schermo un messaggio che informa l'utente. In questo caso occorre rivolgersi al rivenditore presso il quale si è acquistato il programma per ulteriori informazioni.

3.2.2.5. Selezione di un file chiave di licenza

Se si dispone di un file chiave di licenza per Kaspersky Internet Security 7.0, la procedura guidata chiede se si desidera installarlo. Se sì, servirsi del pulsante **Sfoglia** per selezionare il percorso del file della chiave di licenza, riconoscibile dall'estensione *.key,* nella finestra di selezione.

Al termine della procedura di installazione della chiave, nella parte inferiore della finestra vengono visualizzate tutte le informazioni relative alla licenza. il nome dell'utente a cui è intestata la registrazione del software, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della chiave.

3.2.2.6. Completamento dell'attivazione del programma

La procedura di impostazione guidata informa l'utente che il programma è stato attivato correttamente. Vengono visualizzate inoltre informazioni relative alla chiave di licenza installata: il nome dell'utente a cui è intestata la registrazione del software, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della licenza.

3.2.3. Selezione della modalità di sicurezza

In questa finestra, la procedura guidata chiede di selezionare la modalità di sicurezza con la quale funzionerà il programma:

Protezione di base: Sono le impostazioni di default utili per gli utenti che non hanno dimestichezza con i computer o i software anti-virus. Indica che i componenti dell'applicazione sono impostati al livello di protezione

consigliato e che l'utente viene informato solo a proposito di eventi pericolosi (come il riconoscimento di oggetti ed attività pericolose).

Protezione interattiva: Questa modalità offre una protezione dei dati del computer più personalizzata rispetto alla modalità Base. Essa è in grado di intercettare tentativi di modifica delle impostazioni di sistema, attività sospette a livello di sistema e attività non autorizzate a livello di rete.

Tutte le attività sopra elencate possono indicare la presenza di programmi nocivi o semplicemente dipendere da attività standard di programmi in uso sul computer. Spetta all'utente stabilire per ogni singolo caso se consentire o bloccare tali attività.

Se si sceglie questa modalità, occorre specificare quando applicarla:

- **Abilita Modalità apprendimento del firewall** – Richiede l'intervento dell'utente quando programmi installati sul computer tentano di collegarsi a una data risorsa di rete. L'utente può permettere o bloccare tale connessione e configurare una regola Firewall per quel programma. Se si disabilita la modalità Training, il Firewall sarà attivato con le impostzioni di protezione minime e concederà pertanto l'accesso alle risorse di rete a tutte le applicazioni.
- **Abilita controllo del registro** – chiede l'intervento dell'utente se riscontra un tentativo di alterare il registro di sistema

  Se l'applicazione è installata su un computer dotato di Microsoft Windows XP Professional Edition x64. Microsoft Windows Vista o Microsoft Windows Vista x64 le impostazioni sotto elencate per la modalità interattiva non saranno disponibili.

- **Abilita Controllo integrità applicazione** – chiede che l'utente confermi le azioni intraprese quando i moduli vengono caricati sulle applicazioni da monitorare.
- **Abilita difesa proattiva estesa** – questa modalità analizza tutte le attività sospette delle applicazioni del sistema, compresi l'apertura di un browser con impostazioni di riga di comando, inserimenti in processi di applicazioni e intercettori di hook di finestre (disabilitati per impostazione predefinita).

3.2.4. Configurazione delle impostazioni di aggiornamento

La sicurezza del computer dipende direttamente dall'aggiornamento regolare degli firme delle minacce e dei moduli del programma. In questa finestra, la

procedura guidata chiede di selezionare una modalità di aggiornamento del programma e di configurare un piano di aggiornamento.

- **Automatico**. Kaspersky Internet Security copia e installa gli aggiornamenti man mano che vengono messi a disposizione sui server di aggiornamento. È la modalità predefinita.
- **Ogni 1 giorno/i**. Gli aggiornamenti vengono eseguiti automaticamente in base alla programmazione impostata. Per configurare la programmazione fare clic su **Cambia**.
- **Manuale**. Questa opzione consente di eseguire manualmente gli aggiornamenti.

Osservare che, al momento dell'installazione del programma, gli elenchi delle minacce e i moduli del programma in dotazione con il software possono essere ormai obsoleti. Per questo motivo si raccomanda di scaricare gli ultimi aggiornamenti del programma. A tal fine, fare clic su **Aggiorna ora**. Kaspersky Internet Security scarica quindi gli aggiornamenti necessari dai server remoti dedicati e li installa sul computer.

Per configurare gli aggiornamenti (impostare le proprietà di rete, selezionare la risorsa da cui scaricare gli aggiornamenti o il server di aggiornamento più vicino), fare clic su **Impostazioni**.

3.2.5. Programmazione delle scansioni antivirus

La scansione di aree selezionate del computer in cerca di oggetti nocivi è una delle fasi più importanti della protezione del computer.

Al momento dell'installazione di Kaspersky Internet Security, vengono create tre attività di scansione antivirus predefinite. In questa finestra, viene richiesto di scegliere un'impostazione per l'attività di scansione:

Esamina oggetti di avvio

Per impostazione predefinita, Kaspersky Internet Security scansiona gli oggetti di avvio automaticamente ogni volta che viene avviato. Le impostazioni di scansione programmata possono essere modificate in un'altra finestra facendo clic su **Cambia…**.

Esamina aree critiche

Per eseguire automaticamente la scansione antivirus delle aree critiche del computer (memoria di sistema, oggetti di avvio, settori del disco, cartelle di sistema di Windows) selezionare la casella corrispondente. Per configurare la scansione programmata fare clic su **Cambia...**.

Per impostazione predefinita, questa scansione automatica è disabilitata.

Analizza risorse del computer

Per eseguire automaticamente una scansione completa del computer, selezionare la casella appropriata. Per configurare la programmazione fare clic su **Cambia…**.

Per impostazione predefinita, l'esecuzione programmata di questa attività è disabilitata. Tuttavia, si raccomanda di eseguire una scansione completa del computer subito dopo l'installazione del programma.

3.2.6. Restrizioni di accesso al programma

Poiché è possibile che più persone facciano uso di uno stesso computer (famigliari, per esempio) senza essere necessariamente utenti avanzati, e poiché programmi nocivi possono disabilitare la protezione, esiste un'opzione di protezione dell'accesso a Kaspersky Anti-Virus mediante password. L'uso di una password è utile per proteggere il programma da tentativi non autorizzati di disabilitare la protezione o modificare le impostazioni.

Per abilitare la protezione tramite password, selezionare **Abilita protezione tramite password** e completa i campi **Nuova password** e **Conferma password**.

Selezionare sotto l'area alla quale si desidera applicare la protezione tramite password:

Tutte le operazioni (ad eccezione delle notifiche di eventi pericolosi). Richiede la password se l'utente cerca di eseguire qualsiasi azione con il programma, ad eccezione delle risposte alle notifiche in caso di rilevamento di oggetti pericolosi.

Operazioni selezionate:

- **Modifica delle impostazioni dell'applicazione** – richiede la password quando un utente cerca di salvare delle modifiche alle impostazioni del programma.
- **Uscita dal programma in esecuzione** – richiede la password se un utente cerca di chiudere il programma.
- **Arresto/sospensione dei componenti di protezione o delle operazioni di scansione** – richiede la password se l'utente cerca di sospendere o disabilitare completamente un componente di protezione in tempo reale o attività di scansione antivirus.

3.2.7. Controllo Integrità dell'Applicazione

In questa fase la procedura guidata analizzerà le applicazioni installate sul computer (librerie file dinamici, firme digitali di produzione), conterà la somma dei file dell'applicazione e creerà un elenco di programmi che possono essere sicuri dal punto di vista della sicurezza. Ad esempio questo elenco includerà automaticamente tutte le applicazioni firmate digitalmente da Microsoft.

Nel futuro Kaspersky Internet Security utilizzerà le informazioni ottenute mentre analizza la struttura dell'applicazione per prevenire che codici maligni possano essere inseriti nei moduli dell'applicazione.

L'analisi delle applicazioni installate sul computer può richiedere un certo tempo.

3.2.8. Configurazione delle impostazioni di Firewall

Firewall è il componente di Kaspersky Internet Security che protegge il computer sulle reti locali e su Internet. In questa fase, la procedura guidata chiede all'utente di creare un elenco di regole che definiscono il comportamento del Firewall nell'analisi dell'attività di rete del computer.

3.2.8.1. Determinazione dello stato di una zona di sicurezza

In questa fase, la procedura guidata analizza l'ambiente di rete del computer. In base a questa analisi, l'intero spazio di rete viene suddiviso in zone:

Internet – il World Wide Web. In questa zona, Kaspersky Internet Security agisce come una firewall personale. Così facendo, le regole predefinite di filtro pacchetti e delle applicazioni regolano l'intera attività di rete per garantire la massima sicurezza. Durante una sessione di lavoro in questa zona non è possibile modificare le impostazioni di protezione ma solo abilitare la modalità invisibile per una maggiore sicurezza del computer.

Zone di sicurezza – alcune zone, per lo più sottoreti delle quali fa parte il computer (per esempio sottoreti a casa o al lavoro). Per impostazione predefinita, queste zone sono definite "a medio rischio". È possibile modificare lo stato di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtro pacchetti e le applicazioni.

Tutte le zone individuate vengono visualizzate in un elenco. Ciascuna di esse è accompagnata da una descrizione, dalla maschera dell'indirizzo e della sottorete, e dallo stato con il quale ogni determinata attività di rete sarà autorizzata o bloccata da Firewall.

- **Internet**. È lo stato predefinito assegnato a Internet, poiché durante la navigazione il computer è soggetto a tutti i tipi di minacce potenziali. Questo stato è raccomandato anche per le reti non protette da programmi antivirus, firewall, filtri, ecc. Selezionando questo stato, il programma garantisce la massima sicurezza durante l'uso di questa zona, in particolare:

  - Blocco di qualsiasi attività di rete NetBios all'interno della sottorete.
  - Regole di blocco per applicazioni e filtro pacchetti che consentono un'attività NetBios all'interno della sottorete.

  Anche se è stata creata una directory ad accesso libero, le informazioni in essa contenute saranno disponibili solo agli utenti di sottoreti con questo stato. Inoltre, quando si seleziona questo stato, non è possibile accedere a file e stampanti di altre reti di computer.

- **Rete locale**. Il programma assegna questo stato alla maggior parte delle zone di sicurezza rilevate durante l'analisi dell'ambiente di rete del computer, con l'**eccezione** delle zone Internet. Si raccomanda di applicare questo stato alle zone caratterizzate da un fattore di rischio medio (per esempio LAN aziendali). Selezionando questo stato, il programma consente:

  - qualsiasi attività di rete NetBios all'interno della sottorete;
  - regole per applicazioni e filtro pacchetti che consentono un'attività NetBios all'interno della sottorete.

  Selezionare questo stato se si desidera garantire l'accesso a determinate cartelle del computer, bloccando al tempo stesso qualsiasi altra attività esterna.

- **Attendibile** – una rete che si ritiene assolutamente sicura per il computer, il quale non è soggetto ad attacchi e tentativi di accesso ai dati durante la sua presenza in tale rete. In questo caso, ogni attività di rete è consentita. Anche se in precedenza si è selezionato il massimo livello di protezione creando regole di blocco, questi sistemi di sicurezza non vengono applicati per i computer remoti provenienti da una rete affidabile.

Per una maggiore sicurezza durante l'uso di reti indicate come **LAN** o **Internet** è possibile attivare la *modalità invisibile*. Questa funzione consente esclusivamente le attività di rete avviate da utenti o applicazioni autorizzati. In

altre parole, il computer diventa invisibile per il resto dell'ambiente. Questa modalità non pregiudica le prestazioni del computer su Internet.

La modalità invisibile è sconsigliata se il computer funziona da server (per esempio un server di posta o HTTP). In tal caso infatti i computer che si connettono al server non riuscirebbero a vederlo.

Per modificare lo stato di una zona o abilitare/disabilitare la modalità invisibile, selezionarla dall'elenco e seguire i collegamenti appropriati nel riquadro **Descrizione regola** sotto l'elenco. È possibile eseguire attività simili e modificare indirizzi e maschere di sottoreti nella finestra **Impostazioni rete** che si apre facendo clic su **Modifica**.

È possibile aggiungere una nuova zona all'elenco durante la visualizzazione. A tal fine, fare clic su **Aggiungi**. Firewall cerca le zone disponibili e, se le individua, chiede di selezionare uno stato da assegnare loro. È possibile inoltre aggiungere manualmente nuove zone all'elenco (per esempio se si connette il laptop a una nuova rete). A tal fine, usare il pulsante **Aggiungi** e inserire le informazioni necessarie nella finestra **Impostazioni rete**.

Attenzione!

Le reti con range di indirizzi simili o più ampi possono nascondere altre reti. Le reti nascoste possono essere solo rilevabili automaticamente. Qualora in elenco compaia una rete con un range indirizzi più ampio, tutte le reti nascoste aggiunte manualmente dall'utente saranno rimosse. Tutte le impostazioni configurate per la rete più ampia saranno "ereditate" dalle reti nascoste. In caso di rimozione di una rete più ampia, le reti nascoste si separano e ereditano le impostazioni correnti.

Per eliminare una rete dall'elenco, fare clic sul pulsante **Elimina**.

3.2.8.2. Creazione di un elenco di applicazioni di rete

La procedura di configurazione guidata analizza il software installato sul computer e crea un elenco di applicazioni che usano una connessione di rete.

Firewall crea una regola volta a controllare l'attività di rete per ciascuna di queste applicazioni. Le regole vengono applicate in base a modelli per applicazioni comuni che usano connessioni di rete, creati da Kaspersky Lab e in dotazione con il software.

È possibile visualizzare l'elenco delle applicazioni di rete e le rispettive regole nella finestra delle impostazioni di Firewall, accessibile facendo clic su **Applicazioni**.

Per una maggiore sicurezza, è possibile disabilitare la funzione di cache DNS durante l'uso di risorse Internet. Questa funzione riduce drasticamente il tempo di connessione del computer alla risorsa Internet necessaria; al tempo stesso rappresenta però una pericolosa vulnerabilità, sfruttando la quale gli hacker possono creare falle di dati non individuabili per mezzo della firewall. Per questo motivo, per aumentare il livello di sicurezza del computer, si raccomanda di disabilitare la funzione di cache DNS.

3.2.9. Utilizzo della posta in uscita per l'apprendimento di Anti-Spam

In questa fase della procedura guidata, avviene l'apprendimento di Anti-Spam utilizzando i messaggi di posta elettronica in uscita dell'account dell'utente. A tal fine saranno analizzate la cartella **Posta inviata** e relative sottocartelle di Microsoft Office Outlook o Microsoft Outlook Express (client di posta di Windows). Questa analisi aggiorna i database di Anti-Spam e l'elenco di indirizzi consentiti con i risultati dell'apprendimento.

Per arrestare l'apprendimento di Anti-Spam, fare clic sul tasto **Arresta**. Solo i risultati dell'apprendimento raccolti prima di fare clic sul pulsante saranno aggiunti al database di Anti-Spam.

Nota: non sarà possibile tornare all'apprendimento se questo era stato interrotto o se sono stati usati i pulsanti **Avanti/Indietro** della procedura guidata per navigare in altre finestre.

3.2.10. Completamento della procedura guidata

L'ultima finestra della procedura guidata chiede di riavviare il computer per completare l'installazione del programma. Occorre riavviare affinché i driver di Kaspersky Internet Security vengano registrati.

È possibile posticipare il riavvio del computer, ma in tal caso alcuni componenti di protezione del programma non saranno attivi.

3.3. Installazione del programma dal prompt di comando

Per installare Kaspersky Internet Security, immettere quanto segue nel prompt di comando:

```
msiexec /i <package_name>
```

Si avvia la procedura guidata di installazione (vedi 3.1 a pag. 34). Una volta installato il programma, occorre riavviare il computer.

Per installare l'applicazione in modo non interattivo (senza eseguire la procedura guidata), immettere:

```
msiexec /i <package_name> /qn
```

Questa opzione prevede che al termine dell'installazione, il computer venga riavviato automaticamente.

CAPITOLO 4. INTERFACCIA DEL PROGRAMMA

Kaspersky Internet Security è dotato di un'interfaccia semplice e intuitiva. Questo capitolo ne descrive le caratteristiche principali:

- Icona della barra delle applicazioni (vedi 4.1 a pag. 52).
- Menu contestuale (vedi 4.2 a pag. 53).
- Finestra principale (vedi 4.3 a pag. 55).
- Finestra delle impostazioni del programma (vedi 4.4 a pag. 60).

Oltre all'interfaccia principale del programma, vi sono plugin per le seguenti applicazioni:

- Microsoft Office Outlook – scansioni antivirus (vedi 8.2.2 a pag. 114) e scansioni antispam (vedi 13.3.8 a pag. 208).
- Microsoft Outlook Express (vedi 13.3.9 a pag. 211).
- The Bat! – scansioni antivirus (vedi 8.2.3 a pag. 116) e scansioni antispam (vedi 13.3.10 a pag. 213).
- Microsoft Internet Explorer (vedi 12.1.3 a pag. 177).
- Microsoft Windows Explorer (vedi 15.2 a pag. 228).

I plug-in estendono le funzionalità di questi programmi consentendo la gestione e l'impostazione di Kaspersky Internet Security dalle loro interfacce.

4.1. L'icona nell'area di notifica della barra delle applicazioni

Subito dopo l'installazione di Kaspersky Internet Security, nell'area di notifica della barra delle applicazioni viene visualizzata un'icona.

Tale icona che funge da indicatore delle funzioni di Kaspersky Internet Security e riflette lo stato della protezione e mostra una serie di funzioni di base eseguite dal programma.

Se l'icona è attiva (colorata), il computer è protetto. Se l'icona è inattiva (bianco e nero), la protezione è stata disabilitata oppure alcuni dei componenti di protezione (vedi 2.2.1 a pag. 26) sono disattivati.

L'icona di Kaspersky Internet Security cambia in relazione all'operazione eseguita:

- Scansione posta elettronica.
- Scansione degli script.
- Scansione in corso di un file in fase di apertura, salvataggio o esecuzione da parte dell'utente o di un programma.
- Il computer deve essere riavviato affinché gli aggiornamenti diventino effettivi.
- Si è verificato un errore in qualche componente di Kaspersky Internet Security

L'icona consente inoltre di accedere alle funzioni di base dell'interfaccia del programma: il menu contestuale (vedi 4.2 a pag. 53) e la finestra principale (vedi 4.3 a pag. 55).

Per aprire il menu contestuale, fare clic con il pulsante destro del mouse sull'icona del programma.

Per aprire la finestra principale di Kaspersky Internet Security nella sezione **Protezione** (la prima schermata predefinita del programma), fare doppio clic sull'icona del programma. Se si fa clic una volta sola, la finestra principale si apre sulla sezione che era attiva l'ultima volta che il programma è stato chiuso.

Se sono disponibili news da Kaspersky Lab, nell'area di notifica della barra delle applicazioni compare la seguente icona . Fare doppio clic sull'icona per visualizzare le news nella finestra che si apre.

4.2. Il menu contestuale

È possibile eseguire semplici attività di protezione dal menu contestuale (vedi Figura 1).

Il menu di Kaspersky Internet Security contiene i seguenti elementi:

Analizza risorse del computer – avvia una scansione completa del computer in cerca di oggetti pericolosi. Durante l'operazione vengono esaminati i file di tutte le unità, inclusi i supporti di archiviazione esterni.

Ricerca virus – seleziona gli oggetti e ne esegue la scansione antivirus. L'elenco predefinito contiene una serie di file come quelli della cartella Documenti, la cartella Avvio, i database di posta, tutte le unità del computer, ecc. È possibile aggiungere elementi all'elenco, selezionare file da esaminare e avviare scansioni antivirus.

Aggiornamento – consente di scaricare gli aggiornamenti dei moduli del programma e gli elenchi delle minacce di Kaspersky Internet Security, e di installarli sul computer.

Monitoraggio di rete – consente di visualizzare l'elenco delle connessioni di rete stabilite, delle porte aperte e del traffico.

Blocca traffico di rete – blocca temporaneamente tutte le connessioni di rete del computer. Selezionando questa voce dal menu, il livello di sicurezza di Firewall (vedi 12.1.1.1 a pag. 160) si commuterà su **Blocca tutto**. Se si desidera che il computer interagisca ripetutamente con la rete, selezionare questa voce dal menu contestuale.

Attiva – serve per attivare il programma. Occorre attivare la propria versione di Kaspersky Internet Security per ottenere los tato di utente registrato che consente pieno accesso a tutte le funzionalità dell'applicazione e al Supporto Tecnico. Questa voce di menu è disponibile solo se il programma non è attivato.

Impostazioni – consente di visualizzare e configurare le impostazioni di Kaspersky Internet Security.

Apri Kaspersky Internet Security 7.0 – apre la finestra principale del programma (vedi 4.3 a pag. 55).

Sospendi protezione – disabilita temporaneamente o abilita i componenti di protezione in tempo reale del programma (vedi 2.2.1 a pag. 26). Questa voce di menu non influisce sugli aggiornamenti del programma o sulle attività di scansione antivirus.

Informazioni sul programma – richiama una finestra contenente informazioni su Kaspersky Internet Security.

Esci – chiude Kaspersky Internet Security (quando questa opzione è selezionata, l'applicazione sarà scaricata dalla RAM del computer).

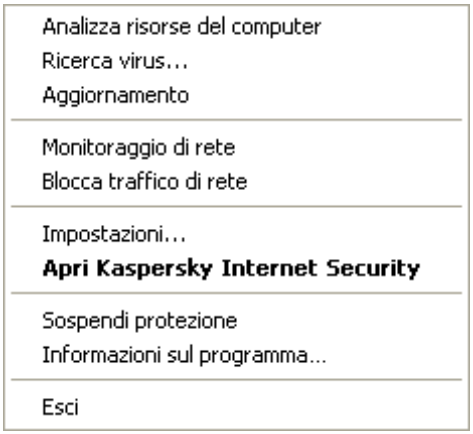


Figura 1. Il menu contestuale

Durante un'attività di scansione antivirus, il menu contestuale visualizza il nome dell'attività accompagnato da un indicatore della percentuale di avanzamento. Selezionando l'attività, è possibile portarsi sulla finestra dei report per visualizzare i risultati correnti.

4.3. La finestra principale del programma

La finestra principale di Kaspersky Internet Security (vedi Figura 2) può essere logicamente suddivisa in tre parti:

- La parte superiore della finestra indica lo stato corrente di protezione del computer.

  Esistono tre possibili stati di protezione (vedi 5.1 a pag. 62), ciascuno con la propria codifica colore, analogamente a un semaforo. Il verde indica che il computer è correttamente protetto, mentre il giallo e il rosso indicano vari problemi di configurazione o funzionamento di Kaspersky Internet Security.

  Per ottenere dettagliate informazioni di risoluzioe guasti e una veloce eliminazione delle anomalie di funzionamento, utilizzare la procedura guidata di sicurezza che si apre facendo clic sul link di notifica di una minaccia.

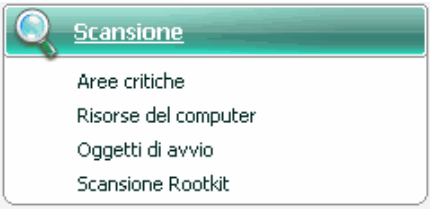
Figura 2. Finestra principale di Kaspersky Internet Security

- *Il pannello di navigazione (parte sinistra della finestra)*, consente di aprire in maniera semplice e veloce qualsiasi componente e di visualizzare i risultati di scansioni antivirus o gli strumenti di supporto del programma;
- La parte destra della finestra, il *pannello informativo,* contiene informazioni sul componente di protezione selezionato nella parte sinistra della finestra e visualizza le impostazioni dei componenti, fornendo gli strumenti per effettuare scansioni antivirus, lavorare con i file in quarantena e le copie di backup, gestire le chiavi di licenza, ecc.

Dopo aver selezionato una sezione o un componente nella parte sinistra della finestra, nella parte destra vengono visualizzate le informazioni relative alla selezione.

Esaminiamo adesso gli elementi del pannello di navigazione della finestra principale.

Sezione della finestra principale	Scopo
	Lo scopo principale della sezione **Protezione** è quello di poter accedere ai componenti di base di protezione in tempo reale del computer. Per visualizzare lo stato di un componente di protezione o relativi moduli, configurarne le impostazioni o aprire un report pertinente, selezionare tale componente dall'elenco sotto **Protezione**. Questa sezione contiene inoltre dei link per accedere alle più comuni attività: scansione anti-virus, e aggiornamento dei database dell'applicazione. Da qui è possibile visualizzare informazioni sullo stato di tali attività, configurarle o eseguirle.

	La sezione **Scansione** consente di accedere alle attività di scansione anti-virus per gli oggetti. Presenta attività di scansione create dagli esperti di Kaspersky Lab, (scansione anti-virus delle aree critiche, degli oggetti di avvio, delle risorse del computer, dei rootkit), oltre che attività per l'utente. Selezionando un'attività dal pannello di destra, vengono visualizzate le informazioni pertinenti, è possibile configurare le impostazioni dell'attività, viene generato un elenco degli oggetti da analizzare, o viene eseguita l'attività. Per scansionare un singolo oggetto (file, cartella o unità), selezionare **Scansione**, usare il pannello di destra per aggiungere l'oggetto all'elenco di quelli da analizzare e lanciare l'attività. Inoltre, questa sezione può essere utilizzata per creare un disco di emergenza (vedi 19.4 a pag. 287).
	La sezione **Aggiornamento** contiene informazioni sugli aggiornamenti dell'applicazione: data di pubblicazione dei database e numero dei tipi di virus riconosciuti. I link appropriati possono essere utilizzati per lanciare un aggiornamento, visualizzare un report dettagliato, configurare gli aggiornamenti, ritornare alla versione precedente l'aggiornamento.

	La sezione **Report e file dati** consente di visualizzare un report dettagliato su ogni componente dell'applicazione, scansione anti-virus o attività di aggiornamento (vedi 19.3 a pag. 269), e lavorare con gli oggetti nelle aree Quarantena (vedi 19.1 a pag. 263) o Backup (vedi 19.2 a pag. 266).
	La sezione **Attivazione** consente di gestire le chiavi necessarie affinché l'applicazione sia pienamente funzionale (vedi Capitolo 18 a pag. 260). Se una chiave non è installata, si raccomanda di acquistarla al più presto e di attivare l'applicazione (vedi 3.2.2 a pag. 40). Se è già stata installata una chiave, questa sezione mostra informazioni sul tipo di chiave utilizzata e sulla relativa data di scadenza. Quando la chiave corrente scade, può essere rinnovata sul sito web di Kaspersky Lab.
	La sezione **Supporto** fornisce informazioni sul Supporto Tecnico disponibile per gli uteni registrati di Kaspersky Internet Security.

Ogni elemento del pannello di navigazione è accompagnato da uno speciale menu contestuale. Esso contiene punti per i componenti di protezione e strumenti che agevolano l'utente nella configurazione e gestione dei componenti e nella visualizzazione dei report. Esiste un'ulteriore voce di menu per le attività di scansione antivirus, utilizzabile per creare un'attività personalizzata, modificando una copia di un'attività esistente.

È possibile anche modificare l'aspetto del programma creando e utilizzando una grafica e uno schema cromatico personalizzati.

Sul lato inferiore sinistro della finestra si trovano due pulsanti: **Guida**, che consente di accedere alla guida di Kaspersky Internet Security e **Impostazioni**, dal quale si apre la finestra delle impostazioni dell'applicazione.

4.4. Finestra delle impostazioni del programma

La finestra delle impostazioni di Kaspersky Internet Security (vedi 4.3 a pag. 55) può essere aperta dalla finestra principale, o dal menu contestuale dell'applicazione (vedi 4.2 a pag. 53).

Fare clic su **Impostazioni** nella sezione inferiore della finestra principale o selezionare l'opzione appropriata nel menu contestuale dell'applicazione.

La finestra delle impostazioni (vedi Figura 3) ha la stessa struttura della finestra principale:

- La parte sinistra della finestra consente di accedere in maniera facile e veloce alle impostazioni di ciascun componente del programma, agli aggiornamenti, alle attività di scansione antivirus e alle impostazioni dell'applicazione;
- La parte destra della finestra contiene un elenco dettagliato delle impostazioni della voce selezionata nella parte sinistra della finestra.

Quando si seleziona qualsiasi sezione, componente o attività nella parte sinistra della finestra delle impostazioni, la parte destra ne visualizza le impostazioni di base. Per configurare le impostazioni avanzate, è possibile aprire le finestre delle impostazioni di secondo e terzo livello. Per una descrizione dettagliata delle impostazioni del programma, consultare le sezioni corrispondenti del manuale dell'utente.

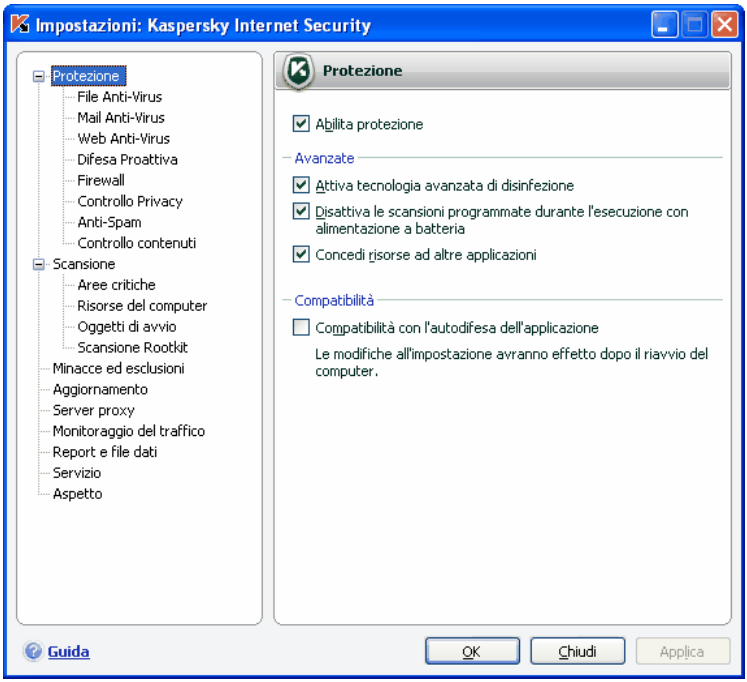


Figura 3. La finestra delle impostazioni di Kaspersky Internet Security

CAPITOLO 5. GUIDA INTRODUTTIVA

Uno dei principali obiettivi di Kaspersky Lab con Kaspersky Internet Security era fornire una configurazione ottimale per tutte le opzioni del programma. Ciò consente agli utenti con qualsiasi livello di conoscenza del computer di proteggere il PC subito dopo l'installazione.

È possibile tuttavia che il computer o il tipo di lavoro per il quale lo si utilizza richiedano delle configurazioni specifiche. Ecco perché si raccomanda di eseguire una configurazione preliminare in modo da ottenere l'approccio più flessibile e personalizzato possibile alla protezione del computer.

Per facilitare al massimo l'attivazione del programma, abbiamo combinato tutte le fasi di configurazione preliminare in una procedura di configurazione guidata (vedi 3.2 a pag. 39) che si avvia al termine dell'installazione del programma. Seguendo le istruzioni della procedura guidata è possibile attivare il programma, configurare le impostazioni degli aggiornamenti e delle scansioni antivirus, proteggere l'accesso al programma mediante password e configurare Firewall in modo da soddisfare i requisiti della rete.

Dopo aver installato e avviato il programma, si raccomanda di eseguire i seguenti passaggi:

- Controllare lo stato corrente della protezione (vedi 5.1 a pag. 62) per garantire che Kaspersky Internet Security funzioni al livello appropriato.
- Eseguire l'apprendimento di Anti-Spam (vedi 5.6 a pag. 68) utilizzando le proprie e-mail.
- Aggiornare il programma (vedi 5.7 a pag. 69) se la procedura guidata non ha provveduto automaticamente dopo l'installazione del programma.
- Eseguire la scansione antivirus del computer (vedi 5.3 a pag. 65).

5.1. Cos'è lo stato di protezione del computer

Lo stato di protezione del computer è una rappresentazione grafica della presenza o dell'assenza di minacce per la sicurezza complessiva del sistema in un dato momento. Ai fini del presente documento, con il termine minacce si intendono sia il software nocivo che i database obsoleti dell'applicazione, la

disattivazione di alcuni componenti di protezione, l'uso delle impostazioni minime dell'applicazione, ecc.

Lo stato della protezione è illustrato in alto nella finestra principale dell'applicazione con colori simili a quelli di un semaforo. In funzione della situazione il colore della parte superiore varia e nel caso di riscontro di minacce oltre al colore verranno aggiunti messaggi informativi, come i link alla procedura guidata di sicurezza.

I seguenti colori vengono utilizzati per mostrare lo stato della protezione:

- La finestra principale dell'applicazione è *verde*. Indica che il computer è correttamente protetto.

  Ciò significa che i database sono regolarmente aggiornati, tutti componenti della protezione sono attivati, l'applicazione è avviata con le impostazioni consigliate degli specialisti di Kaspersky Lab, nessun oggetto nocivo è stato individuato dalla scansione completa del computer o tale oggetto è stato neutralizzato.

- La finestra principale dell'applicazione è *gialla*. La protezione del computer si è abbassata. Questo stato è indicativo di alcuni problemi per l'applicazione o le sue impostazioni.

  Per esempio, sono presenti alcune piccole discrepanze rispetto alla modalità di funzionamento, e i database dell'applicazione non sono stati aggiornati da parecchi giorni, l'addestramento di Anti-Spam non è stato eseguito.

- La finestra principale dell'applicazione è r*ossa*. Avverte a proposito di problemi che potrebbero causare infezioni e perdite di dati. Ad esempio uno o più componenti hanno fallito, il prodotto non è stato aggiornato da molto tempo oppure oggetti pericolosi sono stati individuati ed è necessario rimuoverli urgentemente, o il programma non è stato attivato.

Se si riscontrano problemi nel sistema di protezione raccomandiamo di intervenire immediatamente. Utilizzare la procedura guidata di sicurezza accessibile cliccando sulla notifica delle minacce. Questa procedura guiderà l'utente attraverso tutte le minacce e fornirà le indicazioni per rimuoverle. La criticità della minaccia è segnalata dal colore dell'indicatore:

 - *l'indicatore attira l'attenzione su minacce non critiche* che comunque potrebbero abbassare il livello di protezione del computer. Tenere in considerazione i consigli degli specialisti di Kaspersky Lab.

 - *l'indicatore avverte della presenza di serie minacce* per la sicurezza del computer. Seguire attentamente i consigli seguenti. Sono tutti volti a

migliorare la protezione del computer. Le azioni consigliate sono fornite come link.

Per muoversi nell'elenco delle minacce cliccare sul pulsante Avanti. Viene fornita una dettagliata descrizione di ciascuna minaccia e sono disponibili le seguenti azioni:

- *Elimina immediatamente*. Utilizzando il corrispondente link è possibile eliminare direttamente la minaccia. Per informazioni più approfondite dell'evento, si può consultare il file del report. L'azione consigliata è quella di eliminare subito la minaccia.
- *Rimanda*. Se per qualsiasi ragione non è possibile eliminare subito la minaccia è possibile rimandare questa azione. Usa il collegamento Rimanda.

  Notare che questa opzione non è disponibile per minacce gravi, come ad esempio oggetti che non possono venir disinfettati, crash dei componenti o database dei program file danneggiati.

Se persistono delle minacce anche dopo aver eseguito la procedura guidata di sicurezza una nota apparirà nella parte alta della finestra principale avvertendo l'utente della necessità di eliminarle. Riaprendo la procedura guidata di sicurezza, le minacce posposte non figureranno tra le minacce attive. In ogni caso è ancora possibile visualizzare ed eliminare le minacce il cui trattamento è stato rimandato cliccando sul link Visualizza le minacce il cui trattamento è stato rimandato nella finestra finale della procedura guidata.

Stato protezione visualizza lo stato corrente della protezione del computer per mezzo di speciali indicatori (vedi 5.2 a pag. 62). Le Statistiche contengono i dati relativi all'operazione corrente del programma.

5.2. Verifica dello stato di ciascun componente di protezione

Per conoscere lo stato corrente di ciascun componente di protezione in tempo reale, aprire la finestra principale dell'applicazione e selezionare il componente desiderato sotto **Protezione**. Sulla destra verrà presentato un riepilogo delle informazioni relative al componente selezionato.

Lo stato del componente è l'indicatore più importante:

- *<nome componente> in esecuzione* – la protezione fornita dal componente è al livello desiderato.
- *<nome componente> in sospeso* – il componente è disabilitato per un certo periodo di tempo. Si riavvierà automaticamente dopo l'intervallo di

tempo specificato o al riavvio dell'applicazione. Il componente può essere riavviato manualmente. Cliccare su Ripristina funzionamento.

- <*nome componente*> – *Disattivato*. l'utente ha arrestato il componente. La protezione può essere riavviata ciccando su Abilita.
- <*nome componente*> *disabilitato (errore)* – disabilitato in seguito ad un errore.
- <*nome componente*> *: disattivato* – la protezione fornita dal componente in questione non è disponibile per qualche ragione.

  Se in un componente si verifica un errore, tentare di riavviarlo. Se il riavvio determina ancora un errore, consultare il report relativo al componente che potrebbe contenere le ragioni dell'errore. In caso di mancata risoluzione del problema, salvare il report del componente come file usando **Azioni… → Salva con nome…** e contattare il supporto tecnico di Kaspersky Lab.

Lo stato del componente dovrebbe essere seguito dalle informazioni circa le sue impostazioni (ad esempio livello di protezione, azioni da intraprendere per gli oggetti pericolosi). Se il componente è composto da più moduli, sono presentati gli stati dei moduli: abilitato o disabilitato. Per modificare le impostazioni correnti cliccare su Configura.

Inoltre, vengono fornite le statistiche di funzionamento di alcuni componenti. Cliccare su Apri report per vedere un report dettagliato.

Se per una qualsiasi ragione un componente è in un certo momento messo in pausa o arrestato i risultati al momento di questa azione possono essere visti cliccando su Apri ultimo report di avvio.

5.3. Come eseguire la scansione antivirus del computer

Dopo l'installazione, il programma comunica all'utente con un messaggio nella parte inferiore a sinistra della finestra dell'applicazione che il computer non è ancora stato esaminato e raccomanda di eseguire immediatamente una scansione antivirus.

Kaspersky Internet Security include un'attività di scansione delle risorse del computer, che si trova nella sezione **Scansione** della finestra principale del programma nella.

Cliccando su **Risorse del computer** vengono presentate le impostazioni delle azioni; livello di sicurezza corrente, azioni da intraprendere per oggetti pericolosi. E' anche disponibile un report dell'ultima scansione.

Per eseguire la scansione del computer in cerca di programmi nocivi,

1. Selezionare **Risorse del computer** sotto **Scansione** nella finestra principale dell'applicazione.
2. Cliccare sul link Avvia scansione.

Il programma avvia la scansione del computer visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.4. Come eseguire la scansione di aree critiche del computer

Vi sono aree del computer particolarmente critiche dal punto di vista della sicurezza. Esse sono prese di mira dai programmi nocivi volti a danneggiare il sistema operativo, il processore, la memoria, ecc.

È estremamente importante garantire la sicurezza di queste aree per il corretto funzionamento del computer. Abbiamo quindi programmato un'attività di scansione antivirus specifica per queste aree. Essa si trova nella finestra principale del programma nella sezione **Scansione**.

Selezionando **Aree Critiche** verranno presentate le impostazioni: livello di protezione corrente, azioni da intraprendere. è anche possibile selezionare quale area critica analizzare e scansionare subito queste aree.

Per eseguire la scansione delle aree critiche del computer in cerca di programmi nocivi,

1. Selezionare **Aree Critiche** sotto **Scansione** nella finestra principale dell'applicazione.
2. Cliccare sul link Avvia scansione.

Il programma avvia la scansione delle aree selezionate visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.5. Come eseguire la scansione antivirus di un file, una cartella o un disco

Vi sono situazioni in è necessario eseguire la scansione antivirus di singoli oggetti anziché dell'intero computer, per esempio del disco fisso in cui si trovano programmi, giochi, database di posta portati a casa dall'ufficio, file archiviati ricevuti come allegati, ecc. È possibile selezionare l'oggetto da esaminare per mezzo degli strumenti standard del sistema operativo Windows (per esempio dalla finestra di **Explorer** o dal **Desktop**, ecc.).

Per eseguire la scansione di un oggetto,

posizionare il cursore sopra al nome dell'oggetto selezionato, aprire il menu contestuale di Windows facendo clic con il pulsante destro del mouse e selezionare **Avvia** (vedi Figura 4).

Figura 4. Scansione di un oggetto selezionato utilizzando il menu sensibile al contesto standard di Microsoft Windows

Il programma avvia la scansione dell'oggetto selezionato visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.6. Apprendimento di Anti-Spam

Un passaggio fondamentale per rendere operativo il programma è istruire Anti-Spam a elaborare le e-mail e filtrare la posta spazzatura. Per Spam, si intende posta indesiderata, benché sia difficile stabilire cosa costituisca o meno spam per un dato utente. Se da un lato esistono categorie di messaggi che possono essere definiti spam con un alto grado di precisione e generalità (per esempio e-mail di massa, pubblicità), altre e-mail potrebbero appartenere alla casella di posta in entrata di un utente.

Pertanto, il programma chiede all'utente di stabilire autonomamente quali e-mail considerare spam e quali no. Kaspersky Internet Security chiederà dopo l'installazione se si vuole intraprendere l'apprendimento di Anti-Spam per istruirlo a differenziare tra spam e e-mail accettate. Questa operazione può essere eseguita mediante pulsanti speciali che si inseriscono nel proprio client di posta (Microsoft Office Outlook, Microsoft Outlook Express (programmi di posta di Windows), The Bat!) o utilizzando la speciale procedura guidata di apprendimento.

Per effettuare l'apprendimento di Anti-Spam utilizzando i pulsanti del plug-in del client di posta,

1. Aprire il client di posta predefinito del proprio computer (per es. Microsoft Office Outlook). Sulla barra strumenti sono presenti due pulsanti: **Spam** e **Non Spam**.
2. Selezionare una e-mail accettata o gruppo di e-mail che contengono messaggi accettati e fare clic su **Non Spam**. Da questo momento in poi, le e-mail provenienti dagli indirizzi selezionati non saranno mai elaborati come spam.
3. Selezionare un'e-mail, un gruppo di e-mail o una cartella di e-mail che si considera spam, e fare clic su **Spam**. Anti-Spam analizzerà I contenuti di queste e-mail e in futuro considererà tutti i messaggi con simili contenuti come spam.

Per effettuare l'apprendimento di Anti-Spam utilizzando la procedura guidata:

Selezionare il componente **Anti-Spam** sotto **Protezione** nel pannello sinistro della finestra principale dell'applicazione e fare clic su Avvia Esercitazione guidata (vedi 13.2.1 a pag. 192).

Quando una e-mail arriva nella casella di posta in entrata, Anti-Spam la analizzerà per verificare la presenza di contenuti spam e aggiungerà uno speciale tag [Spam] nella riga dell'oggetto. È possibile configurare una speciale regola nel proprio client di posta per questi messaggi, come una regola secondo la quale tali e-mail devono essere eliminate o trasferite in una cartella particolare.

5.7. Come aggiornare il programma

Kaspersky Lab aggiorna gli elenchi delle minacce di Kaspersky Internet Security e i moduli del programma per mezzo di appositi server di aggiornamento.

I server di aggiornamento di Kaspersky Lab sono siti Internet di Kaspersky Lab Internet in cui vengono archiviati gli aggiornamenti dei programmi.

Attenzione!

Per aggiornare Kaspersky Internet Security è necessario disporre di un collegamento Internet.

Come impostazione predefinita, Kaspersky Internet Security verifica automaticamente la presenza di aggiornamenti sui server di Kaspersky Lab. Se Kaspersky Lab ha reso pubblici degli aggiornamenti del programma, Kaspersky Internet Security li scarica e li installa in modalità invisibile.

Per aggiornare Kaspersky Internet Security manualmente,

1. Selezionare la sezione **Aggiornamento** nella finestra principale dell'applicazione.
2. Fare clic su Aggiorna database.

Kaspersky Internet Security avvia così il processo di aggiornamento. Tutti i dettagli del processo vengono visualizzati in un'apposita finestra.

5.8. Cosa fare se la protezione non funziona

Se si verificano problemi o errori di funzionamento di qualsiasi componente di protezione, è bene verificarne lo stato. Se lo stato del componente è *disabilitato o in esecuzione (errore di sottosistema)* cercare di riavviare il programma.

Se il problema non si risolve dopo aver riavviato il programma, si raccomanda di correggere potenziali errori utilizzando la funzione di ripristino dell'applicazione (**Start → Programmi → Kaspersky Internet Security 7.0 → Modifica, ripara o rimuovi**).

Se la procedura di ripristino non produce risultati contattare il Supporto Tecnico di Kaspersky Lab. Potrebbe essere necessario salvare in un file il report sul funzionamento del componente e inviarlo al Supporto Tecnico per successive analisi.

Per salvare il report su un file:

1. Selezionare il componente nella sezione **Protezione** della finestra principale del programma e fare clic su Apri report (componente correntemente attivo) oppure Apri ultimo report di avvio (per un componente disabilitato).
2. Nella finestra del report cliccare su **Azioni… → Salva con nome…** e nella finestra che si apre, specificare il nome del file in cui il report sarà salvato.

CAPITOLO 6. SISTEMA DI GESTIONE DELLA PROTEZIONE

Questa sezione fornisce informazioni su come configurare le impostazioni comuni usate dai componenti di protezione in tempo reale dell'applicazione e dalle attività, oltre a informazioni circa la creazione di specifici ambiti di protezione, elenchi di minacce da gestire, e di un elenco di oggetti attendibili che possono essere ignorati dalla protezione:

- gestione in tempo reale della protezione (vedi 6.1 a pag. 71);
- utilizzo della Tecnologia avanzata di disinfezione (vedi 6.2 a pag. 75);
- esecuzione di attività su un portatile (vedi 6.3 a pag. 76);
- cooperazione di Kaspersky Internet Security con altre applicazioni (vedi 6.4 a pg. 76);
- compatibilità di Kaspersky Internet Security con caratteristiche di auto-difesa di altre applicazioni (vedi 6.5 a pag. 77);
- elenco delle protezioni da minacce (vedi 6.8 a pag. 81) di cui è fornita l'applicazione;
- elenco degli oggetti attendibili (vedi 6.9 a pag. 82) che verranno ignorati dalla protezione.

6.1. Interruzione e ripristino della protezione in tempo reale del computer

Per impostazione predefinita, Kaspersky Internet Security viene caricato all'avvio del sistema e protegge il computer per tutto il tempo che resta in uso. Il messaggio *Kaspersky Internet Security 7.0* nell'angolo superiore destro dello schermo informa l'utente che tutti i componenti di protezione (vedi 2.2.1 a pag. 26) sono in funzione.

È possibile disabilitare completamente o parzialmente la protezione offerta da Kaspersky Internet Security.

Attenzione!

Kaspersky Lab raccomanda caldamente di **non disabilitare la protezione in tempo reale**, poiché ciò potrebbe provocare l'infezione del computer, con conseguente perdita di dati.

Osservare che in questo caso la protezione è descritta nel contesto dei componenti di protezione. Disabilitare o sospendere i componenti di protezione non pregiudica le prestazioni delle attività di scansione antivirus o aggiornamento del programma.

6.1.1. Sospensione della protezione

Sospendere la protezione in tempo reale significa disabilitare temporaneamente tutti i componenti di protezione che monitorano i file del computer, la posta in arrivo e in uscita, gli script eseguibili, il comportamento delle applicazioni, Firewall, Anti-Spam e Controllo contenuti.

Per sospendere la protezione in tempo reale del computer:

1. Selezionare **Sospendi** nel menu contestuale del programma (vedi 4.2 a pag. 53).
2. Nella finestra che si apre (vedi Figura 5), specificare quando si desidera ripristinare la protezione:
   - Tra <intervallo di tempo> **-** la protezione sarà ripristinata dopo questo intervallo. Per selezionare un valore usa il menu a discesa.
   - Al prossimo riavvio del programma – la protezione sarà ripristinata aprendo il programma dal menu **Start** o dopo aver riavviato il computer (a condizione che il programma sia impostato in modo da aprirsi automaticamente all'avvio (vedi 19.11 a pag. 310).
   - Solo su richiesta dell'utente – la protezione si arresterà fino ad un nuovo comando di avvio. Per abilitare la protezione selezione **Riprendi protezione** dal menu contestuale del programma.

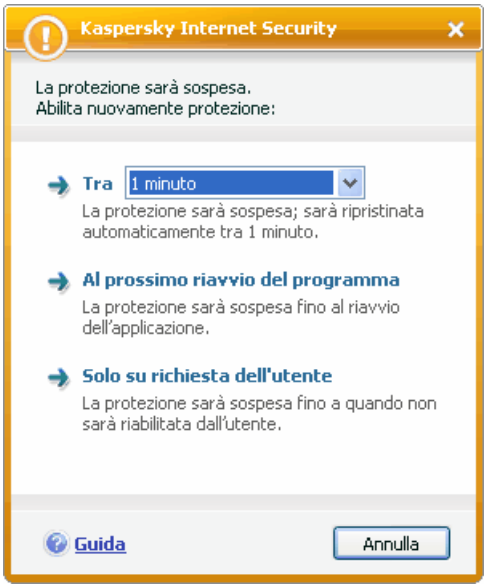


Figura 5. Finestra di sospensione della protezione

Se metti in pausa la protezione lo saranno anche tutti i suoi componenti in tempo reale. Questo è indicato da:

- Nomi dei componenti inattivi (in grigio) nella sezione **Protezione** della finestra principale.
- Icona inattiva (in grigio) nell'area di notifica della barra delle applicazioni.

6.1.2. Interruzione della protezione

Interrompere la protezione significa disabilitare completamente i componenti di protezione in tempo reale. Le attività di scansione antivirus e di aggiornamento continuano a funzionare in questa modalità.

Se la protezione è interrotta, essa può essere ripristinata esclusivamente dall'utente: i suoi componenti non si ripristinano automaticamente al riavvio del sistema o del programma. Ricordare che se Kaspersky Internet Security è in conflitto con altri programmi installati sul computer, è possibile sospendere i singoli componenti o creare un elenco di esclusioni (vedi 6.9 a pag. 82).

Per interrompere completamente a protezione in tempo reale:

1. Aprire la finestra principale di Kaspersky Internet Security e selezionare **Protezione**.
2. Deselezionare **Abilita protezione**.

Disabilitando la protezione, tutti i suoi componenti si interrompono. Questo stato è indicato da:

- Nomi inattivi (di colore grigio) dei componenti disabilitati nella sezione **Protezione** della finestra principale.
- Icona inattiva (di colore grigio) nell'area di notifica della barra delle applicazioni.

6.1.3. Sospensione/interruzione di singoli componenti di protezione

Esistono molti modi per interrompere un componente di protezione, una scansione antivirus o un aggiornamento. Tuttavia, prima di farlo, si raccomanda di stabilire per quale motivo si desidera interromperli. È probabile infatti che esista una soluzione diversa al problema, per esempio modificare il livello di sicurezza. Se, per esempio, si lavora con un database che sicuramente non contiene virus, è sufficiente aggiungerne i file tra le esclusioni (vedi 6.9 a pag. 82).

Per sospendere un singolo componente della protezione:

Aprire la finestra principale e selezionare il componente sotto **Protezione** e cliccare su Sospendi.

Lo stato del componente/attività diventa sospeso. Il componente o attività resterà sospeso fino a quando l'utente li ripristinerà facendo clic sul link Riprendi protezione.

Quando si mette in pausa un componente, vengono salvate le statistiche della corrente sessione di Kaspersky Internet Security e restano disponibili fino a che il componente viene aggiornato.

Per interrompere un singolo componente della protezione:

Aprire la finestra principale e selezionare il componente sotto **Protezione** e cliccare su Interrompi.

Lo stato del componente diventa *Disattivato,* mentre il nome del componente diventa inattivo sotto **Protezione** (grigio). Il componente resterà interrotto fino a quando l'utente li abiliterà facendo clic sul Abilita.

Ogni componente di protezione può venir arrestato anche dalla finestra delle impostazioni dell'applicazione. Aprire la finestra delle impostazioni, selezionare il componente sotto **Protezione** e deselezionare ☑ **Abilita <nome del componente>**

Quando si disabilita un componente di protezione tutte le statistiche vengono azzerate e ricominciate al riavvio del componente.

I singoli componenti di protezione vengono disabilitati anche arrestando la protezione in tempo reale del computer (vedi 6.1.2 a pag. 73).

6.1.4. Ripristino della protezione del computer

Se l'utente ha sospeso o interrotto la protezione del computer, potrà ripristinarla mediante uno dei seguenti metodi:

- *Dal menu contestuale*.

  Selezionare **Riprendi protezione**.

- *Dalla finestra principale del programma*.

  Seleziona la sezione **Protezione** nella parte sinistra della finestra principale e cliccare su Abilita protezione.

Lo stato della protezione diventa immediatamente *attivo*. L'icona del programma nell'area di notifica della barra delle applicazioni diventa attiva (colorata).

6.2. Tecnologia avanzata di disinfezione

Malware sofisticati possono infiltrarsi nei bassi livelli del sistema operativo rendendo impossibile la loro rimozione. Quando viene scoperto un pericolo sul sistema Kaspersky Internet Security suggerisce una speciale ed estesa procedura di disinfezione che disabilita e rimuove le minacce dal computer.

Completata la procedura il computer dovrà essere riavviato. Si consiglia di avviare una completa scansione del computer dopo il riavvio. Per avviare la procedura di Disinfezione Avanzata aprire la finestra delle impostazioni, selezionare **Protezione** e spuntare ☑ **Attiva tecnologia avanzata di disinfezione** (vedi Figura 6).

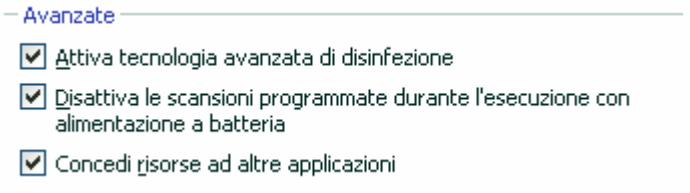


Figura 6. Configurazione delle impostazioni più diffuse

6.3. Esecuzione dell'applicazione su computer portatili

Su un computer portatile, le attività di scansione possono essere posticipate per non esaurire le batterie.

Poiché la scansione del computer d il suo frequente aggiornamento assorbono significative risorse e tempo, consigliamo di programmare queste attività. Ciò permetterà di salvaguardare la durata delle batterie. Sarà possibile aggiornare l'applicazione (vedi 5.7 a pag. 69) o lanciare una scansione anti-virus (vedi 5.3 a pag. 65) manualmente. Per salvaguardare la durata delle batterie aprire la finestra delle impostazioni, selezionare **Protezione** e spuntare **Disattiva le scansioni programmate durante l'esecuzione con alimentazione a batteria** (vedi Figura 6) sotto **Avanzate.**

6.4. Prestazioni del computer con l'applicazione in esecuzione

Per limitare il carico della CPU e dei sottosistemi di memoria, le scansioni possono essere posticipate.

La scansione anti-virus incrementa il carico della CPU e del sottosistema abbassando la velocità di esecuzione di altri programmi. Se questo avviene il programma sospende per impostazione predefinita la scansione anti-virus e concede parte delle risorse alle applicazioni dell'utente.

Ci sono però programmi che si avviano non appena le risorse della CPU sono disponibili e lavorano in background. Per rendere indipendente la scansione anti-virus da questi programmi aprire la finestra delle impostazioni dell'applicazione, selezionare **Protezione** e spunta **Concedi risorse ad altre applicazioni** (vedi Figura 6) in **Avanzate**.

Notare che questo parametro può essere configurato per ogni singola attività di scansione anti-virus. L'impostazione per ogni singola attività avrà una più elevata priorità.

6.5. Risoluzione di problemi di compatibilità tra Kaspersky Internet Security e altre applicazioni

L'esecuzione di Kaspersky Internet Security può talvolta generare conflitti con altre applicazioni installate. Ciò è dovuto al fatto che tali applicazioni sono dotate di un meccanismo di autodifesa incorporato che viene attivato da Kaspersky Internet Security quando tenta di integrarsi. Queste applicazioni incorporano plug-in di Autenticazione per Adobe Reader, che verifica l'accesso ai documenti Pdf, Oxigen Phone Manager II la gestione dei cellulari, oltre ad alcuni giochi tamper-proof.

Per risolvere questi inconvenienti, aprire la finestra delle impostazioni dell'applicazione, selezionare **Protezione** e spuntare **Compatibilità con l'autodifesa dell'applicazione** sotto **Compatibilità** (vedi Figura 7). Perché questa impostazione abbia effetto occorre riavviare il sistema operativo.

Si noti tuttavia, che quando questa opzione è selezionata, I moduli di Controllo contenuti (Anti-Dialer e Protezione di dati riservati), oltre al plugin di Anti-Spam per Microsoft Outlook Express non funzionano. Quando questi moduli sono attivati, la modalità di compatibilità viene disabilitata automaticamente. Tuttavia, questi moduli non funzioneranno fino al prossimo avvio dell'applicazione.

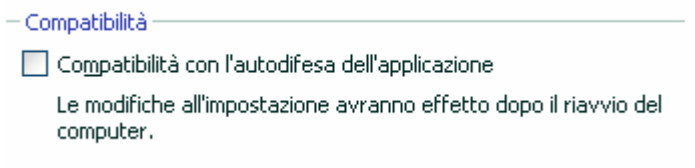


Figura 7. Configurazione delle impostazioni di compatibilità

Attenzione!

Se l'applicazione è installata su un computer con sistema operativo Microsoft Windows Vista e Microsoft Windows Vista x64, la risoluzione dei problemi di compatibilità con i meccanismi di autodifesa di altre applicazioni non è supportata.

6.6. Avvio di attività di scansione antivirus e aggiornamento utilizzando un diverso account

Kaspersky Internet Security 7.0 è dotato di una funzione che consente di avviare le attività sotto un altro account. Questa funzione è normalmente disabilitata e le attività vengono eseguite con l'account con cui l'utente si collega al sistema.

Questa funzione è utile se per esempio durante una scansione occorrono determinati privilegi di accesso. Utilizzando questa funzione, è possibile configurare attività da eseguire con l'account di un utente in possesso dei privilegi richiesti.

È possibile che gli aggiornamenti del programma debbano essere eseguiti da un'origine alla quale non si ha accesso (per esempio la cartella aggiornamenti di rete) o da un server proxy per il quale non si hanno diritti. È possibile quindi utilizzare questa funzione per eseguire l'aggiornamento utilizzando un account in possesso dei diritti necessari.

Per configurare un'attività di scansione da eseguire con un account utente diverso:

1. Aprire la finestra impostazioni dell'applicazione e selezionare l'attività sotto **Scansione**.
2. Fare clic sul pulsante **Personalizza…** nel **Livello di protezione** ed aprire la scheda **Avanzate** nella finestra di dialogo che si apre.

Per configurare un'attività di aggiornamento da eseguire con un profilo utente diverso:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Aggiornamento**.
2. Fare clic sul pulsante **Configura** sotto **Impostazioni aggiornamento** ed aprire la scheda **Avanzate** nella finestra di dialogo (vedi Figura 8).

Per abilitare questa funzione, selezionare la casella **Esegui questa attività come**. Inserire i dati di login del profilo con cui si desidera avviare l'attività: nome utente e password.

Si noti che, se la funzione Esegui questa attività come non è abilitata, gli aggiornamenti programmati avverranno in accordo con l'utente corrente. Nel caso che nessuno sia registrato nel sistema e tale opzione non sia configurata, un aggiornamento programmato si avvierà come SISTEMA.

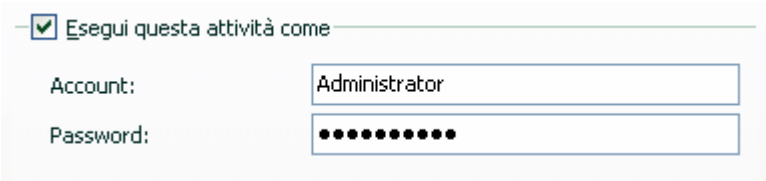


Figura 8. Configurazione di un'attività di aggiornamento da un altro account utente

6.7. Configurazione di azioni programmate e notifiche

La configurazione della programmazione è identica per le attività di scansione anti-virus, aggiornamento dell'applicazione e messaggi di funzionamento di Kaspersky Internet Security.

Per impostazione predefinita, sono disabilitate le attività di scansione create durante l'installazione. L'unica eccezione è la scansione degli oggetti di avvio che avviene ogni volta che si avvia Kaspersky Internet Security. Gli aggiornamenti sono configurati per essere eseguiti automaticamente non appena un aggiornamento è disponibile sui server di Kaspersky Lab.

Qualora queste impostazioni non siano soddisfacenti per l'utente, la pianificazione può essere modificata.

Figura 9. Creazione del piano di esecuzione delle attività

Il primo valore da definire è la frequenza di un evento (esecuzione o notifica). Seleziona l'opzione desiderata sotto **Frequenza** (vedi Figura 9). Poi occorre specificare sotto **Pianificazione: Aggiornamento** l'impostazione di aggiornamento per l'opzione selezionata. Sono disponibili le seguenti selezioni:

Il primo valore da definire è la frequenza di un evento (esecuzione o notifica). Seleziona l'opzione desiderata sotto **Frequenza** (vedi Figura 9). Poi occorre specificare sotto **Pianificazione: Aggiornamento** l'impostazione di aggiornamento per l'opzione selezionata. Sono disponibili le seguenti selezioni:

- **A un'ora specificata**. L'azione si avvia o viene spedita la notifica alla data ed all'ora specificata.
- **All'avvio dell'applicazione**. L'azione si avvia o viene spedita la notifica ogni volta che viene avviato Kaspersky Anti-Virus. E' anche possibile specificare un ritardo dall'avvio dell'applicazione.
- **Dopo ogni aggiornamento**, L'evento si avvia dopo l'aggiornamento del database dell'applicazione (opzione valida solo per le scansioni).
- **Ogni minuto**. L'intervallo di esecuzione dell'evento è definito in minuti. Impostare i minuti. Non è possibile può superare i 59 minuti.
- **Ore**. L'intervallo di esecuzione dell'evento è definito in ore. Impostare le ore in **OGNI N ore** e impostare **N**. Ad esempio **OGNI 1 ora**.
- **Giorni**. L'intervallo di esecuzione dell'evento è definito in giorni. Impostare i giorni:
  - Selezionare **OGNI N giorni** e specifica N.
  - Selezionare **Ogni giorno feriale** se desideri che l'azione avvenga da Lunedì a Venerdì.
  - Selezionare **Ogni fine settimana** per avviare l'azione il sabato e la domenica.

Usare il campo **Ora** per specificare l'ora di avvio dell'azione.

- **Settimane**. Le attività saranno eseguite o le notifiche inviate in un dato certo giorno della settimana. Per selezionare questa frequenza, spuntare i giorni corrispondenti nelle impostazioni di pianificazione. Usare il campo **Ora** per definire l'ora del lancio.
- **Ogni mese**. Le attività saranno eseguite o le notifiche inviate una volta al mese all'ora specificata.

Se una azione non riesce ad avviarsi (ad esempio non è installato un programma di posta elettronica oppure il computer è spento in quel momento), può essere configurata in modo che venga lanciata automaticamente non appena possibile. Spuntare nella finestra di pianificazione ☑ **Esegui attività se saltata**.

6.8. Tipi di Malware da monitorare

Kaspersky Internet Security protegge da diversi tipi di programmi pericolosi. Indipendentemente dalle impostazioni il programma protegge sempre il computer dai tipi di malware più pericolosi, come virus, trojan ed hack tool. Questi programmi possono causare significativi danni al computer. Per migliorare la sicurezza del computer è possibile estendere l'elenco delle minacce che il programma intercetterà facendogli monitorare ulteriori tipi di programmi pericolosi.

Per scegliere da quali programmi pericolosi Kaspersky Internet Security proteggerà il computer, selezionare la finestra delle impostazioni di programma e selezionare **Minacce ed Esclusioni** (vedi Figura 10).

Il riquadro delle categorie Malware contiene tre tipi di minacce (vedi 1.1 a pag. 11):

- **Virus, worm, Trojan, utilità di hacking**. Questo gruppo comprende le categorie più comuni e pericolose. Questo è il limite minimo ammissibile di sicurezza. Su raccomandazione degli esperti di Kaspersky Lab , Kaspersky Internet Security verifica sempre queste categorie di programmi pericolosi.
- **Spyware, adware, dialer**. Questo gruppo include software potenzialmente pericolosi che possono disturbare l'utente o causare seri danni.
- **Software potenzialmente pericoloso (riskware)**. Questo gruppo include programmi che non sono maligni o pericolosi. In ogni caso, in certe condizioni, potrebbero essere utilizzati per nuocere al computer.

I gruppi sopra riportati comprendono la totalità delle minacce che il programma riconosce durante la scansione degli oggetti.

Se si selezionano tutti i gruppi, Kaspersky Internet Security fornisce la più alta protezione per il computer. Se il secondo e terzo gruppo sono disabilitati il programma proteggerà dai programmi pericolosi più comuni. Questi non comprendono programmi potenzialmente pericolosi ed altri che potrebbero venire installati sul computer e che potrebbero danneggiare i file, sottrarre denaro o far perdere tempo.

Kaspersky Lab consiglia di non disabilitare il monitoraggio del secondo gruppo. Se sorge un problema nel momento in cui Kaspersky Internet Security classifica un programma che l'utente considera attendibile come potenzialmente periocoloso, si consiglia di creare un'esclusione per tale programma (vedi 6.9 a pag. 82).

Per selezionare i tipi di malware da monitorare:

aprire la finestra impostazioni dell'applicazione e selezionare **Minacce ed esclusioni**. La configurazione si esegue nelle **Categorie malware** (vedi Figura 10).

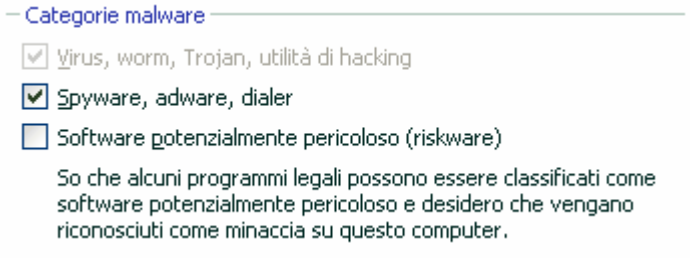


Figura 10. Selezione delle minacce da monitorare

6.9. Creazione di una zona attendibile

Una *zona attendibile* è un elenco di oggetti creato dall'utente, che Kaspersky Internet Security non esamina. In altre parole, si tratta di una serie di programmi esclusi dalla protezione.

L'utente crea una zona protetta sulla base delle proprietà dei file che usa e dei programmi installati sul computer. Questo elenco di esclusioni può tornare utile, per esempio, se Kaspersky Internet Security blocca l'accesso a un oggetto o programma della cui sicurezza l'utente è assolutamente sicuro.

È possibile escludere file dalla scansione in base al formato, oppure usare una maschera, escludere una determinata area (per esempio una cartella o un programma), processi di programmi o oggetti in base allo stato che il programma assegna agli oggetti durante una scansione.

Nota!

Gli oggetti esclusi non sono soggetti a scansione durante l'analisi del disco o della cartella a cui appartengono. Tuttavia, se si seleziona quell'oggetto in particolare, la regola di esclusione non verrà applicata.

Per creare un elenco di esclusioni,

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare la sezione **Minacce ed esclusioni** (vedi Figura 10).
2. Fare clic sul pulsante **Area attendibile…** nella sezione **Esclusioni**.
3. Configurare le regole di esclusione degli oggetti e creare un elenco di applicazioni attendibili nella finestra che si apre (vedi Figura 11).

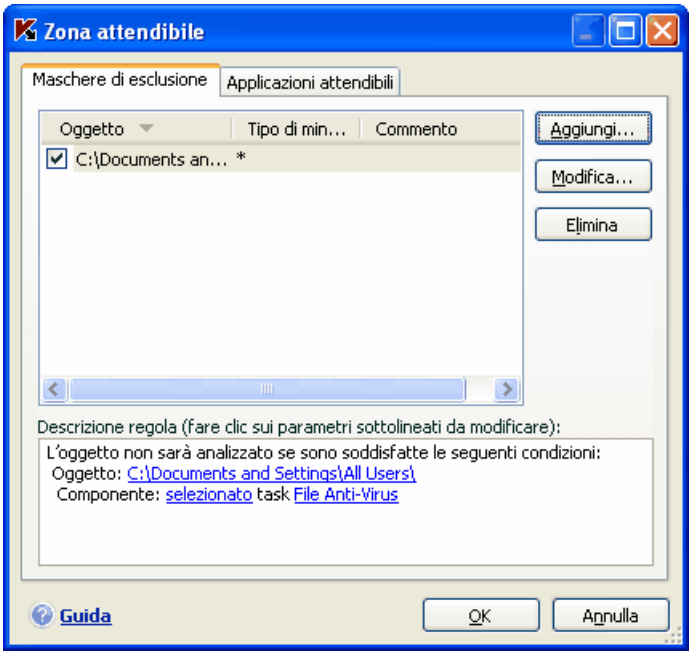


Figura 11. Creazione di una zona attendibile

6.9.1. Regole di esclusione

Le *regole di esclusione* sono delle condizioni in base alle quali Kaspersky Internet Security stabilisce quali oggetti non sottoporre a scansione.

È possibile escludere i file dalla scansione in base al formato, usare una maschera, escludere una determinata area come una cartella o un programma, processi di programmi o oggetti in base alla loro classificazione della Enciclopedia dei tipi di minaccia.

Il *Tipo di Minaccia* à lo stato che Kaspersky Internet Security assegna a un oggetto durante la scansione. Un verdetto si basa sulla classificazione dei programmi nocivi e potenzialmente pericolosi presenti nell'Enciclopedia dei virus di Kaspersky Lab.

Il software potenzialmente pericoloso non svolge una funzione nociva vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. Di questa categoria fanno parte, per esempio, programmi di amministrazione remota, client IRC, servizi FTP, utility multifunzione per interrompere o nascondere i processi,

keylogger, macro per la decodifica di password, autodialer, ecc. Questi programmi non sono classificati come virus. Essi possono essere suddivisi in diverse categorie, per esempio adware, scherzi, riskware, ecc. (per ulteriori informazioni sui programmi potenzialmente pericolosi individuati da Kaspersky Internet Security, vedi Virus Encyclopedia su www.viruslist.com). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di essi sono estremamente comuni, è possibile escluderli dalla scansione. A tal fine, aggiungere il nome della minaccia o maschera alla zona attendibile usando la classificazione dell'Enciclopedia dei virus.

Poniamo per esempio di utilizzare frequentemente un programma di amministrazione remota. Si tratta di un sistema di accesso remoto che consente di lavorare da un altro computer. Kaspersky Internet Security visualizza questo tipo di applicazione come potenzialmente pericolosa e la blocca. Per evitare il blocco dell'applicazione, è necessario creare una regola di esclusione che specifichi *not-a-virus: RemoteAdmin.Win32RAdmin.22* come tipo di minaccia.

Quando si aggiunge un'esclusione, viene creata una regola che in seguito sarà utilizzata da numerosi componenti del programma (File Anti-Virus, Mail Anti-Virus, Difesa proattiva, modulo di Controllo contenuti per la protezione dei dati confidenziali, Web Anti-Virus) e attività di scansione antivirus. Le regole di esclusione, si creano in una finestra specifica accessibile dalla finestra delle impostazioni del programma, dall'avviso di rilevamento dell'oggetto e dalla finestra dei report.

*Per aggiungere esclusioni nella scheda **Maschere di esclusione**:*

1. Fare clic sul pulsante **Aggiungi…** nella scheda **Maschere di esclusione** (vedi Figura 11).
2. Nella finestra che si apre (vedi Figura 12), fare clic sul tipo di esclusione nella sezione **Proprietà**:

   Oggetto – esclusione dalla scansione di un oggetto, directory o file corrispondente a una determinata maschera.

   Tipo di minaccia – esclusione dalla scansione di oggetti in base allo stato assegnato loro dall'Enciclopedia dei virus.

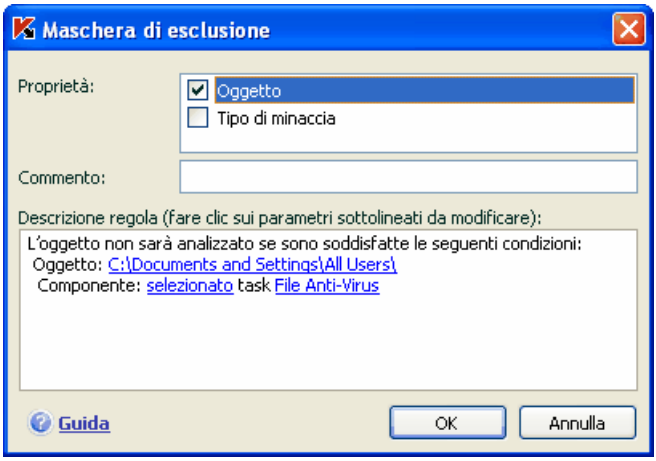


Figura 12. Creazione di una regola di esclusione

Se si selezionano subito entrambe le caselle, si crea una regola con un determinato stato in accordo con la classificazione dell'Enciclopedia dei virus, In tal caso vale la seguente regola:

- Se si specifica un determinato file come **Oggetto** e un determinato stato nella sezione **Tipo di minaccia**, il file specificato sarà escluso solo se classificato come il tipo di minaccia selezionata durante la scansione.
- Se si seleziona un'area o cartella come **Oggetto** e lo stato (o maschera dei verdetti) come **Tipo di minaccia**, gli oggetti con quello stato saranno esclusi solo dalla scansione di quell'area o cartella.

3. Assegnare dei valori ai tipi di esclusione selezionati. A tal fine, fare clic con il pulsante sinistro del mouse nella sezione **Descrizione regola** sul link specifica ubicato a fianco del tipo di esclusione:
   - Per il tipo di oggetto, digitare il nome nella finestra che si apre (può trattarsi di un file, di una directory o di una maschera di file, vedi A.2 a pag. 338). Selezionare ☑ **Includi sottocartelle** per l'oggetto (file, maschera di file, cartella) da escludere ripetutamente dalla scansione. Per esempio, se si specifica **C:\Program Files\winword.exe** come esclusione selezionando l'opzione sottocartelle, il file **winword.exe** sarà escluso dalla scansione se presente in qualsiasi sottocartella di **C:\Programmi**.
   - Digitare il nome completo della minaccia che si desidera escludere dalle scansioni come indicato nell'enciclopedia dei virus, oppure

utilizzare una maschera (vedi A.3 a pag. 338) per il **Tipo di minaccia**.

Per alcuni tipi di minacce, è possibile assegnare condizioni avanzate per l'applicazione di regole nel campo **Impostazioni avanzate**. In molti casi questo campo è compilato automaticamente quando si aggiunge un'esclusione da una notifica di Difesa Proattiva

Tra l'altro puoi aggiungere impostazioni avanzate per le seguenti minacce:

- *Invasore* (inserimento nei processi del programma) Per questa minaccia, si può assegnare un nome, un percorso completo all'oggetto inserito (per esempio un file .dll) come condizione di esclusione supplementare.
- *Lancio del Browser Internet*. Per questa minaccia, si può elencare i dettagli di apertura del browser come impostazioni di esclusione addizionali.

  Per esempio, è possibile bloccare l'apertura dei browser con determinate impostazioni nella finestra di analisi dell'attività di Difesa Proattiva. Tuttavia, si desidera che il browser si apra per il dominio www.kaspersky.it con un link da Microsoft Office Outlook come regola di esclusione. Per fare questo selezionare Microsoft Office Outlook come **Oggetto** e *Lancio del Browser Internet* come **Tipo di Minaccia**, ed inserire una maschera di dominio nel campo **Impostazioni Avanzate**.

4. Definire quali componenti di Kaspersky Internet Security devono applicare questa regola. Se si seleziona qualsiasi, la regola sarà applicata a tutti i componenti. Se si desidera limitare la regola a uno o più componenti, fare clic su qualsiasi che cambia in selezionato. Nella finestra che si apre, selezionare le caselle relative ai componenti ai quali si desidera applicare questa regola di esclusione.

Per creare una regola di esclusione da una notifica che comunica il rilevamento di un oggetto periocoloso:

1. Utilizzare il link Aggiungi a zona attendibile nella finestra della notifica (vedi Figura 13).
2. Nella finestra che si apre, verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dalla notifica. Per creare la regola, fare clic su **OK**.

Per creare una regola di esclusione dalla finestra dei report:

1. Selezionare nel report l'oggetto che si desidera aggiungere alle esclusioni.
2. Aprire il menu contestuale e selezionare **Aggiungi a zona attendibile** (vedi Figura 14).
3. Si apre quindi la finestra delle impostazioni delle esclusioni. Verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dal report. Per creare la regola, fare clic su **OK**.

Figura 13. Notifica del rilevamento di un oggetto pericoloso

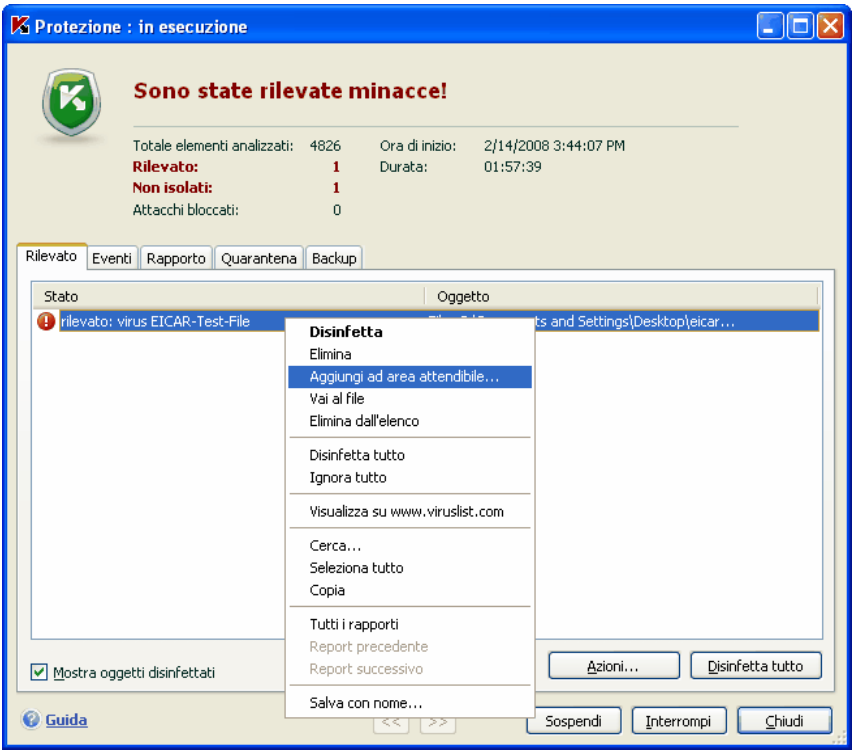


Figura 14. Creazione di una regola di esclusione da un report

6.9.2. Applicazioni attendibili

Kaspersky Internet Security è in grado di creare un elenco di applicazioni attendibili di cui non è necessario monitorare le attività dei loro file o della rete e dell'accesso al registro di sistema.

Per esempio, si può ritenere che gli oggetti utilizzati da Microsoft Windows Notepad siano sicuri e non necessitino di scansione. In altre parole, ci si fida dei processi di questo programma. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere **Notepad** all'elenco delle applicazioni attendibili. Tuttavia, il file eseguibile e il processo dell'applicazione affidabile saranno sottoposti a scansione antivirus come in precedenza. Per escludere completamente l'applicazione dalla scansione, è necessario utilizzare le regole di esclusione (vedi 6.9.1 a pag. 83).

Inoltre, è possibile che alcune azioni classificate come pericolose siano in realtà perfettamente normali per le funzioni di determinati programmi. Per esempio, i programmi di commutazione del layout di tastiera intercettano regolarmente il testo digitato sulla tastiera. Per giustificare le operazioni specifiche di tali programmi ed escludere dal monitoraggio le loro attività, si raccomanda di aggiungerli all'elenco delle applicazioni attendibili.

Grazie alle esclusioni delle applicazioni attendibili è possibile inoltre risolvere potenziali conflitti di compatibilità tra Kaspersky Internet Security e altre applicazioni (per esempio il traffico di rete da un altro computer che è appena stato esaminato dall'applicazione antivirus) e incrementare la produttività del computer, particolarmente importante quando si utilizzano applicazioni server.

Per impostazione predefinita, Kaspersky Internet Security esamina gli oggetti aperti, eseguiti o salvati da qualsiasi processo di programma e monitora l'attività di tutti i programmi e il traffico di rete che creano.

È possibile creare un elenco di applicazioni attendibili nella scheda specifica **Applicazioni attendibili** (vedi Figura 15). L'elenco creato al momento dell'installazione contiene applicazioni sicure la cui attività non verrà controllata come consigliato da Kaspersky Lab. Se non si ritiene sicura un'applicazione dell'elenco deselezionare la casella corrispondente. È possibile aggiungere elementi e modificare l'elenco servendosi dei pulsanti **Aggiungi, Modifica** ed **Elimina** sulla destra.

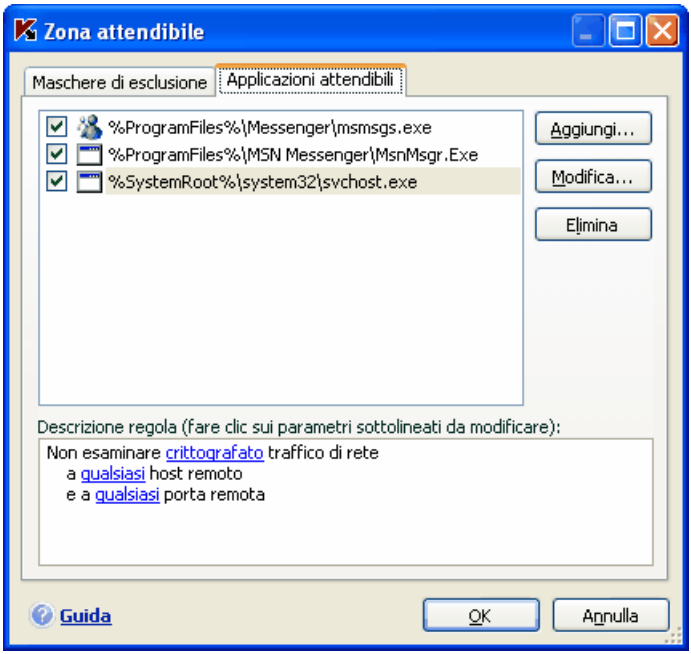


Figura 15. Elenco delle applicazioni attendibili

Per aggiungere un programma all'elenco delle applicazioni attendibili:

1. Fare clic sul pulsante **Aggiungi** nella parte destra della finestra.
2. Nella finestra **Applicazione attendibile** (vedi Figura 16) che si apre, selezionare l'applicazione per mezzo del pulsante **Sfoglia**. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possibile aprire la finestra di selezione dei file e selezionare il percorso del file eseguibile. In alternativa, facendo clic su **Applicazioni** è possibile aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate.

   Quando si seleziona un programma, Kaspersky Internet Security registra gli attributi interni del file eseguibile e li usa per identificare il programma come attendibile durante le scansioni.

   Il percorso del file viene inserito automaticamente quando se ne seleziona il nome. È possibile tuttavia modificarlo manualmente.

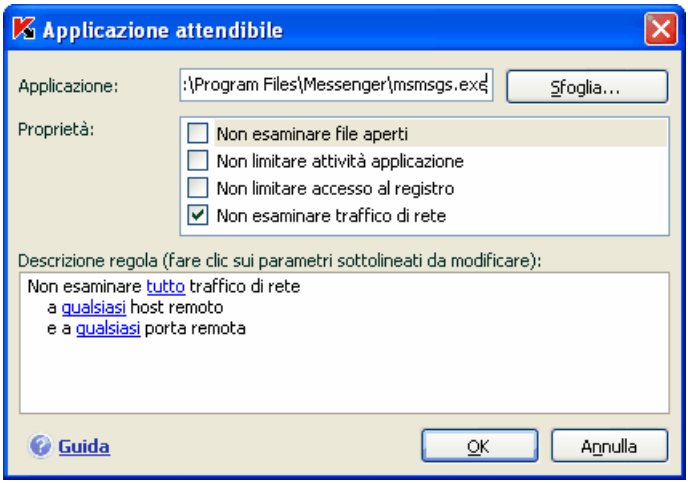


Figura 16. Aggiunta di un'applicazione all'elenco di quelle attendibili

3. Specificare quindi le azioni eseguite da questo processo che Kaspersky Internet Security non deve monitorare:

   - **Non esaminare file aperti** – esclude dalla scansione tutti i file che il processo dell'applicazione attendibile apre.
   - **Non limitare attività applicazione** – esclude dal monitoraggio di Difesa proattiva qualsiasi attività, sospetta o no, che un'applicazione attendibile sta eseguendo.
   - **Non limitare accesso al registro** – esclude dalla scansione i tentativi di accesso al registro di sistema avviati dalle applicazioni attendibili.
   - **Non esaminare traffico di rete** – esclude dalle scansioni antivirus e antispam il traffico di rete avviato dalle applicazioni attendibili. È possibile escludere dalla scansione il traffico di rete o quello protetto (SSL) generato da tali applicazioni. A tal fine, usare il collegamento tutto**.** Questo sarà modificato in crittografato. È inoltre possibile limitare l'esclusione assegnando una porta remota o un host remoto. Per creare una limitazione, fare clic su qualsiasi, che diventa selezionato, e digitare un valore per la porta/host remoto.

Osservare che se la casella **Non esaminare traffico di rete** è selezionata, il traffico relativo all'applicazione sarà sottoposto alla sola scansione antivirus e antispam. Questo tuttavia non influisce sulla scansione del traffico da parte di Firewall. Le impostazioni di Firewall influiscono sull'analisi dell'attività di rete dell'applicazione in questione.

CAPITOLO 7. FILE ANTI-VIRUS

Kaspersky Internet Security contiene un componente speciale per la protezione antivirus dei file presenti nel computer, *File Anti-Virus.* Esso viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer ed esamina tutti i file aperti, salvati o eseguiti.

L'indicatore di funzionamento del componente è l'icona della barra delle applicazioni di Kaspersky Internet Security, che durante la scansione di un file assume questo aspetto  .

Per impostazione predefinita, File Anti-Virus esamina soltanto i *file nuovi o modificati*. In altre parole, esamina i file che sono stati aggiunti o modificati dall'ultimo accesso. I file sono scansionati secondo il seguente algoritmo:

1. Il componente intercetta i tentativi da parte dell'utente o di programmi di accedere a qualsiasi file.
2. File Anti-Virus esamina i database di iChecker™ e iSwift™ in cerca di informazioni sul file intercettato. In base alle informazioni recuperate, si decide se scansionare o meno il file.

Il processo di scansione si svolge come segue:

1. Il file viene sottoposto a scansione antivirus. Gli oggetti nocivi vengono individuati operando un confronto con i database dell'applicazione, che contengono le descrizioni di tutti i programmi nocivi, le minacce e gli attacchi di rete noti nonché dei metodi per neutralizzarli.
2. Dopo l'analisi, esistono le tre seguenti possibili azioni:
    a. In caso di rilevamento di un codice nocivo, File Anti-Virus blocca il file interessato, ne salva una copia nel *Backup* e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene reso nuovamente accessibile. In caso contrario il file viene eliminato. Quando il file viene disinfettato o eliminato, Anti-Virus ne ripone una copia nella cartella *Backup*.
    b. Se Anti-Virus rileva in un file un codice sconosciuto che assomiglia a un codice nocivo ma non vi è certezza in merito, tale file sarà posto in una cartella particolare, *Quarantena.* In un secondo momento, l'utente può cercare di disinfettarlo con i database aggiornati.
    c. Se nel file non viene rilevato alcun codice nocivo, il file viene immediatamente ripristinato.

7.1. Selezione di un livello di sicurezza dei file

File Anti-Virus protegge i file in uso ad uno dei seguenti livelli (vedi Figura 17):

- **Protezione massima** – il livello di monitoraggio più approfondito dei file aperti, salvati o eseguiti.
- **Consigliato** – Kaspersky Lab raccomanda questo livello. Esso esegue la scansione delle seguenti categorie di oggetti:
  - Programmi e file in base ai contenuti.
  - Oggetti nuovi e oggetti modificati dopo l'ultima scansione.
  - Oggetti OLE incorporati.
- **Alta velocità** – livello che consente di utilizzare le applicazioni che richiedono considerevoli risorse di sistema, grazie alla limitazione del numero di file esaminati.

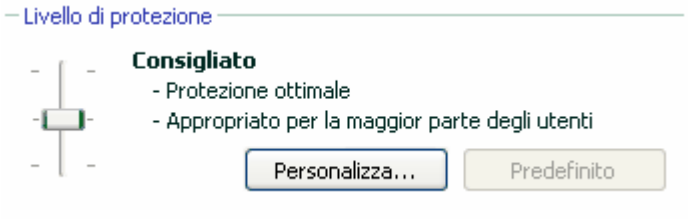


Figura 17. Livello di protezione di File Anti-Virus

Per impostazione predefinita, File Anti-Virus è impostato su **Consigliato**.

È possibile aumentare o ridurre il livello di protezione dei file selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Regolando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di file esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di file esaminati.

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzarne le impostazioni di protezione. A tal fine, selezionare il livello più vicino alle proprie esigenze come punto di partenza, e modificarne le impostazioni. Così facendo, il livello di protezione diventerà personalizzato. Vediamo l'esempio di un caso in cui modificare le impostazioni predefinite del livello di protezione può essere molto utile.

Esempio:

Il lavoro svolto sul computer comporta numerosi di tipi di file, alcuni dei quali di dimensioni piuttosto elevate. L'utente non desidera correre il rischio di omettere dalla scansione eventuali file a causa delle dimensioni o dell'estensione, anche se ciò potrebbe influire sulla produttività del computer.

Suggerimento per selezionare un livello:

In base ai dati sulla provenienza, si potrebbe concludere che il rischio di infezione da parte di un programma nocivo sia piuttosto elevato. Le dimensioni e il tipo dei file gestiti sono molto eterogenei e l'eventuale esclusione di qualsiasi file dalla scansione comporterebbe un rischio elevato per i dati del computer. L'utente desidera esaminare i file utilizzati in base al contenuto, non in base all'estensione.

Si raccomanda quindi di selezionare inizialmente il livello di sicurezza **Consigliato** e di apportare le seguenti modifiche: rimuovere le restrizioni sui file eliminati e ottimizzare il funzionamento di File Anti-Virus esaminando solo i file nuovi e modificati. In tal modo la scansione non influirà eccessivamente sulle risorse di sistema e sarà possibile continuare a usare senza problemi altre applicazioni.

Per modificare le impostazioni di un livello di sicurezza:

1. Aprire la finestra delle impostazioni e selezionare **File Anti-Virus** sotto **Protection**.
2. Fare clic su **Personalizza** sotto **Livello di protezione** (vedi Figura 17).
3. Modificare i parametri di protezione del file nella finestra che si apre e fare clic su **OK**.

7.2. Configurazione di File Anti-Virus

Il modo in cui File Anti-Virus proteggerà il computer su cui è installato dipende dalla configurazione. Le impostazioni del programma possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono i tipi di file (vedi 7.2.1 a pag. 96) da sottoporre alla scansione antivirus.
- Impostazioni che definiscono l'ampiezza della protezione (vedi 7.2.2 a pag. 98).
- Impostazioni che definiscono le reazioni del programma agli oggetti pericolosi individuati (vedi 7.2.6 a pag. 105).

- Impostazioni che definiscono l'uso dei metodi euristici (vedi 7.2.4 a pag. 103).
- Impostazioni avanzate di File Anti-Virus (vedi 7.2.3 a pag. 100).

La presente sezione prende in esame questi gruppi di impostazioni.

7.2.1. Definizione dei tipi di file da esaminare

Selezionando i tipi di file da esaminare, si specificano i formati di file, le dimensioni e le unità da sottoporre alla scansione antivirus all'apertura, esecuzione o salvataggio.

Al fine di agevolare la configurazione, tutti i file sono stati suddivisi in due gruppi: *semplici* e *compositi*. I file semplici non contengono oggetti (per esempio i file .txt). I file compositi possono contenere numerosi oggetti, ciascuno dei quali a sua volta può avere diversi livelli di nidificazione. Gli esempi sono numerosi: archivi, file che contengono macro, fogli di calcolo, e-mail con allegati, ecc.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (vedi Figura 18). Selezionare una delle seguenti opzioni:

Esamina tutti i file. Con questa opzione selezionata tutti gli oggetti del file system che vengono aperti, eseguiti o salvati saranno esaminati senza eccezioni.

Esamina programmi e documenti (in base al contenuto). Se è stato selezionato questo gruppo di file, File Anti-Virus esaminerà solo i file potenzialmente infetti, cioè i file che possono contenere virus.

> **Nota:**
>
> Vi sono formati di file che sono a bassissimo rischio di contenere codici nocivi, e quindi difficilmente un virus può attivarsi in essi, come per esempio i file .txt.

Prima di cercare virus in un file, viene analizzata l'intestazione interna del formato (txt, doc, exe, ecc.). Se dall'analisi risulta che il formato del file non consente infezioni, il file viene escluso dalla scansione e messo immediatamente a disposizione dell'utente. Se il formato file è infettabile, il file viene sottoposto a scansione antivirus.

Esamina programmi e documenti (in base all'estensione). Se è stata selezionata questa opzione, File Anti-Virus esamina solo i file potenzialmente infetti, ma il formato del file sarà determinato dall'estensione. Per mezzo del link estensione, è possibile consultare un elenco delle estensioni (vedi A.1 a pag. 334) esaminate con questa opzione.

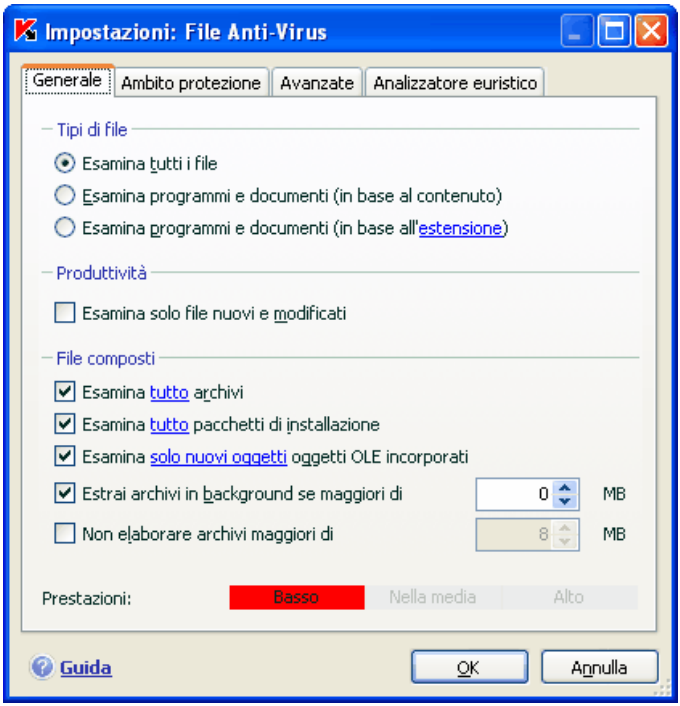


Figura 18. Selezione dei tipi di file sottoposti a scansione antivirus

Suggerimento:

Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Esamina programmi e documenti (in base all'estensione)**, tale file sarebbe escluso dalla scansione. Selezionando invece l'opzione **Esamina programmi e documenti (in base al contenuto)** e ignorando l'estensione, File Anti-Virus analizzerebbe in primo luogo le intestazioni dei file, scoprendo che il falso file .txt è in realtà un file .exe. Il file sarebbe quindi sottoposto a un'approfondita scansione antivirus.

Nella sezione **Produttività**, è possibile specificare che si desidera sottoporre a scansione antivirus i soli file nuovi o modificati. Questa modalità riduce considerevolmente la durata della scansione e aumenta la velocità del programma. Per attivare questa modalità, selezionare la casella **Esamina solo file nuovi e modificati**. Questa modalità si applica sia ai file semplici sia a quelli compositi.

Nella sezione **File composti**, specificare quali file compositi sottoporre alla scansione antivirus:

- **Esamina archivi** – vengono esaminati gli archivi .zip, .cab, .rar, e .arj.
- **Esamina pacchetti di installazione** – vengono sottoposti alla scansione antivirus gli archivi autoestraenti.
- **Esamina oggetti OLE incorporati** – vengono esaminati gli oggetti incorporati all'interno di file (per esempio fogli di calcolo Excel o una macro incorporata in un file di MS Word, allegati alle e-mail, ecc.).

Per ogni tipo di file composito è possibile selezionare ed esaminare tutti i file o solo quelli nuovi usando il link a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Produttività** è stata impostata in modo da esaminare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file composito da sottoporre a scansione.

Per specificare quali file compositi non devono essere sottoposti alla scansione antivirus utilizzare le seguenti impostazioni:

- **Non elaborare archivi maggiori di ... MB**. Se le dimensioni di un oggetto composito superano questo limite, il programma lo esamina come se fosse un oggetto singolo (analizzando l'intestazione) e lo restituisce all'utente. Gli oggetti in esso contenuti saranno esaminati in un secondo momento. Se questa opzione non è stata selezionata, l'accesso ai file di dimensioni superiori sarà bloccato fino a scansione avvenuta.
- **Estrai archivi in background se maggiori di ... MB**. Se è stata selezionata questa opzione, i file di dimensioni superiori a quella specificata saranno esclusi dalla scansione.

7.2.2. Definizione dell'ambito della protezione

File Anti-Virus esamina per impostazione predefinita tutti i file che vengono usati, indipendentemente dalla loro posizione, sia essa un disco fisso, un CD-ROM o un'unità flash.

È possibile limitare l'ambito della protezione procedendo come segue:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **File Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Personalizza…** nell'area Livello di protezione (vedi Figura 17).

3. Selezionare la scheda **Ambito protezione** (vedi Figura 19) nella finestra di dialogo che si apre.

La scheda visualizza un elenco di oggetti che File Anti-Virus analizzerà. La protezione è abilitata per impostazione predefinita per tutti gli oggetti presenti sui dischi fissi, su supporti esterni e su unità di rete connesse al computer. È possibile aggiungere elementi e modificare l'elenco servendosi dei pulsanti **Aggiungi, Modifica** ed **Elimina**.

Se si desidera proteggere un numero minore di oggetti, è possibile procedere come segue:

1. Specificare solo le cartelle, le unità e i file che necessitano di protezione.
2. Creare un elenco di oggetti che non necessitano di protezione.
3. Combinare i metodi uno e due per creare una protezione il cui ambito esclude una serie di oggetti.

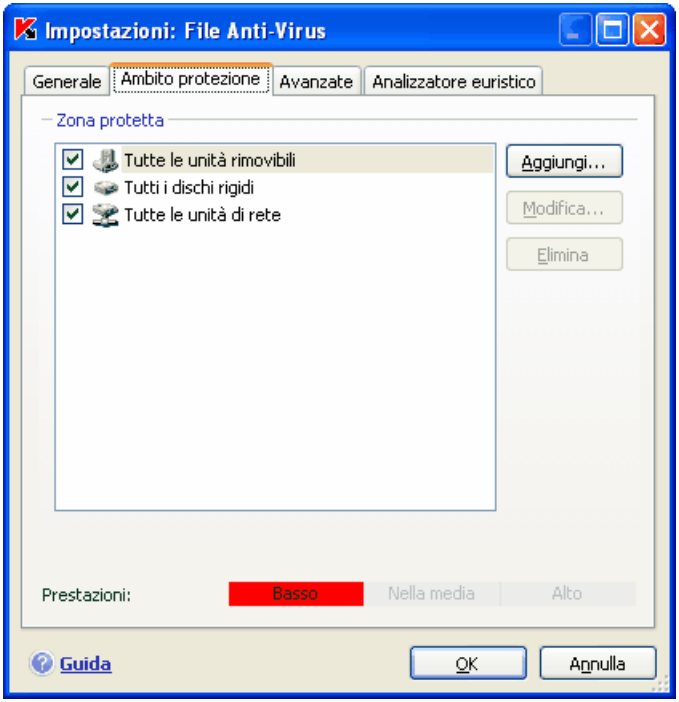


Figura 19. Creazione di una zona protetta

Per aggiungere oggetti al processo di scansione, è possibile utilizzare delle maschere. Tuttavia, è possibile immettere unicamente maschere con percorsi assoluti agli oggetti:

- **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file nella cartella *C:\dir*
- **C:\dir*.exe** – tutti i file con estensione .exe nella cartella *C:\dir*
- **C:\dir*.ex?** – tutti i file con estensione .ex? nella cartella *C:\dir\,* dove ? può rappresentare qualsiasi carattere
- **C:\dir\test** – solo il file *C:\dir\test*

Per eseguire la scansione in modo ripetitivo, selezionare la cartella **Includi sottocartelle**.

Attenzione!

Ricordare che File Anti-Virus esamina solo i file inclusi nell'ambito della protezione creato. I file non inclusi in quell'ambito saranno disponibili per l'uso senza essere sottoposti a scansione antivirus. Ciò incrementa il rischio di infezione del computer.

7.2.3. Configurazione delle impostazioni avanzate

Nelle impostazioni avanzate di File Anti-Virus, è possibile specificare la modalità di scansione del file system, nonché configurare le condizioni per mettere temporaneamente in pausa il componente.

Per configurare le impostazioni avanzate File Anti-Virus:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **File Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Personalizza** nell'area **Livello di protezione** (vedi Figura 17).
3. Selezionare la scheda **Avanzate** nella finestra di dialogo che si apre (vedi Figura 20).

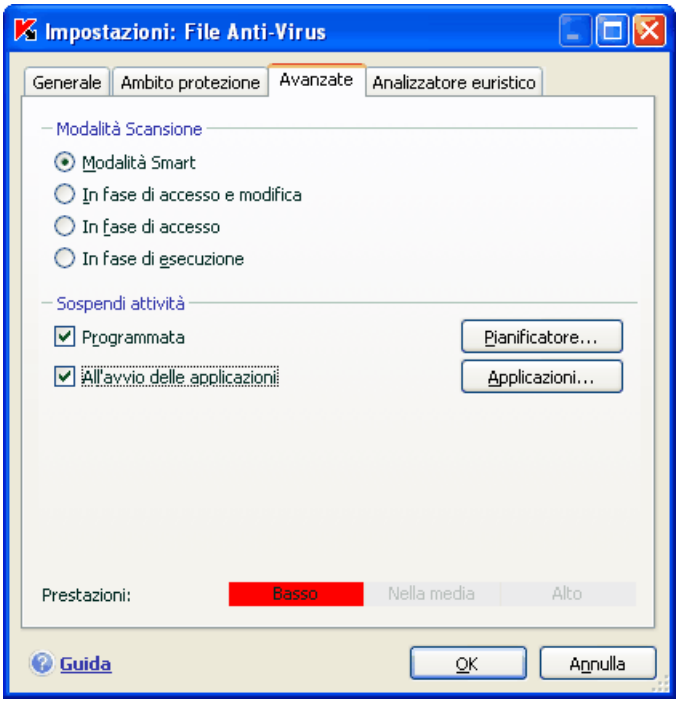


Figura 20. Configurazione delle impostazioni avanzate di File Anti-Virus

La modalità di scansione dei file determina le condizioni di elaborazione File Anti-Virus. Sono disponibili le seguenti opzioni:

- **Modalità Smart**. Questa modalità mira ad accelerare l'elaborazione dei file per restituirli all'utente. Quando è selezionata, la decisione di scansione viene presa analizzando le operazioni eseguite col file.

  Ad esempio, quando si utilizza un file di Microsoft Office, Kaspersky Internet Security esamina il file all'apertura iniziale ed alla chiusura finale. Tutte le operazioni che sovrascrivono il file comprese tra queste due operazioni non vengono esaminate.

  La modalità Smart è quella predefinita.

- **In fase di accesso e modifica** – File Anti-Virus esamina i file quando vengono aperti o modificati.

- **In fase di accesso** – i file vengono esaminati solo quando si cerca di aprirli.

- **In fase di esecuzione** – i file vengono esaminati solo quando si cerca di eseguirli.

Potrebbe essere necessario sospendere l'attività di File Anti-Virus quando si eseguono attività che richiedono una grande quantità di risorse del sistema. Per diminuire il carico e fare in modo che l'utente riottenga rapidamente l'accesso ai file, si consiglia di configurare il componente per la disattivazione ad una certa ora o quando vengono utilizzati determinati programmi.

Per sospendere l'attività del componente per un determinato intervallo di tempo, selezionare **Programmata**, fare clic su **Pianificatore…** e assegnare un intervallo per la disattivazione del componente nella finestra che si apre (vedi Figura 21). A tal fine, inserire una valore in formato HH:MM nei campi corrispondenti.

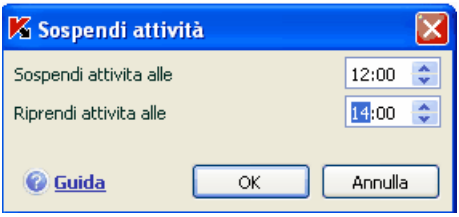


Figura 21. Sospensione dell'attività del componente

Per disattivare il componente quando si lavora con programmi che utilizzano una grande quantità di risorse del sistema, selezionare **All'avvio delle applicazioni** e modificare l'elenco di programmi nella finestra che si apre (vedi (vedi Figura 22) facendo clic su **Applicazioni…**.

Per aggiungere un'applicazione all'elenco, utilizzare il pulsante **Aggiungi…**. Si apre un menu sensibile al contesto, dal quale, facendo clic su **Sfoglia…** si raggiunge la finestra standard di selezione file per specificare il file eseguibile dell'applicazione da aggiungere; oppure, è possibile passare all'elenco delle applicazioni attualmente in esecuzione scegliendo **Applicazioni** e selezionare quella desiderata.

Per eliminare un'applicazione, selezionarla dall'elenco e fare clic su **Elimina**.

È possibile disabilitare temporaneamente la sospensione dell'attività di File Anti-Virus con un'applicazione specifica, deselezionandone il nome. Non è necessario eliminarla dall'elenco.

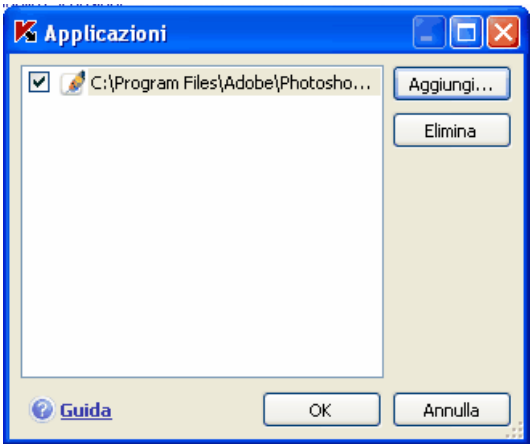


Figura 22. Creazione di un elenco di applicazioni

7.2.4. Utilizzo dell'analizzatore euristico

I metodi euristici sono utilizzati da numerosi componenti di protezione in tempo reale, come File, Mail, Web Anti-Virus così come dalle attività di scansione anti-virus.

Naturalmente la scansione, che usa il metodo delle firme con un database creato precedentemente e che contiene una descrizione delle minacce conosciute e del modo di trattarle, fornirà una risposta definitiva riguardo la pericolosità di un oggetto e indicherà a quale classe di programmi pericolosi esso appartiene. Il metodo euristico, diversamente dal metodo delle firme, è volto a riconoscere comportamenti od operazioni tipiche piuttosto che i codici identificativi pericolosi, grazie ai quali il programma classifica un file con una certa probabilità. Il vantaggio del metodo euristico è che non necessita di database precostituiti per funzionare. Grazie a questo, nuove minacce possono essere riconosciute prima ancora di essere state incontrate dagli analisti.

L'analizzatore euristico simula l'esecuzione dell'oggetto nell'ambiente sicuro e virtuale di Kaspersky Anti-Virus. Se l'oggetto non presenta un comportamento sospetto, la sua esecuzione nell'ambiente operativo è consentita. Se all'esecuzione si riscontra un'attività sospetta, l'oggetto viene classificato come nocivo e la sua esecuzione sull'host sarà bloccata, oppure viene visualizzato un messaggio che richiede l'intervento dell'utente.

- Quarantena. le nuove minacce verranno processate in seguito utilizzando database più aggiornati
- Elimina l'oggetto

- Ignora (se si ritiene che l'oggetto non sia pericoloso)

Per usare il metodo euristico selezionare **Usa analizzatore euristico.** È inoltre possibile selezionare il livello di dettaglio della scansione. A tal fine, spostare il cursore su una delle seguenti opzioni: **Basso, Medio** o **Dettagliato**. In questo modo si può scegliere il livello di completezza e la qualità della scansione per le nuove minacce nei confronti del carico sul sistema operativo e la durata della scansione. Più alto sarà il livello dell'analisi euristica, maggiori saranno le risorse di sistema necessarie che la scansione richiederà e più lunga la sua durata.

Attenzione:

Le nuove minacce rilevate dall'analizzatore euristico sono velocemente analizzate da Kaspersky Lab, e i metodi per neutralizzarle sono aggiunti ai nostri aggiornamenti del database pubblicati a cadenza oraria.

Pertanto, se si aggiornano regolarmente i database dell'applicazione sul computer e i livelli di protezione si mantengono ottimizzati, non è necessario tenere abilitata l'analisi euristica in modo continuativo.

La scheda **Analizzatore euristico** (vedi Figura 23) può essere utilizzata per abilitare/disabilitare l'analisi euristica di File Anti-Virus verso minacce sconosciute. Occorre eseguire i seguenti passaggi:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **File Anti-Virus** sotto **Protezione**.
2. Cliccare sul pulsante **Personalizza…** nell'area del livello di protezione (vedi Figura 17).
3. Selezionare la scheda **Analizzatore euristico** nella finestra di dialogo che si apre.

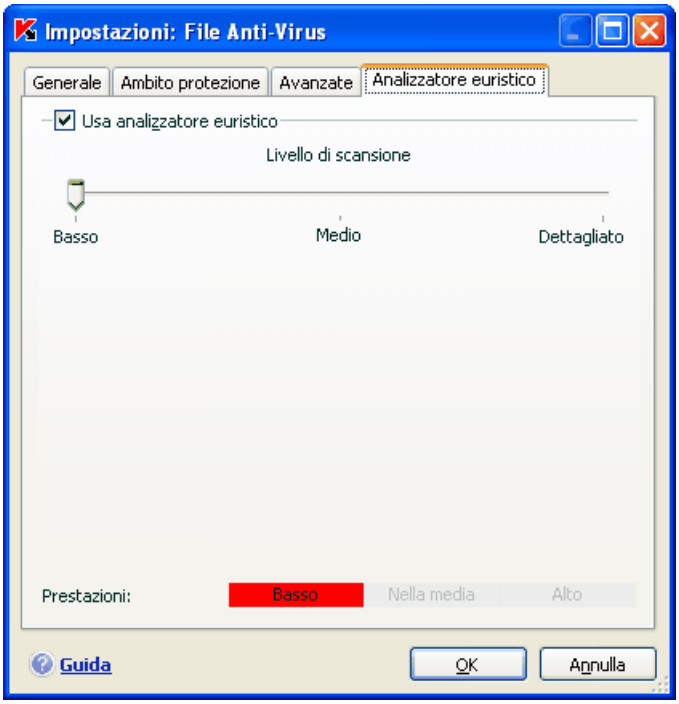


Figura 23. Uso dell'analizzatore euristico

7.2.5. Ripristino delle impostazioni di File Anti-Virus

Durante la configurazione di File Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni predefinite di File Anti-Virus:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **File Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di protezione**.

Se l'elenco degli oggetti inclusi nella zona protetta delle impostazioni di configurazione di File Anti-Virus è stato modificato, il programma chiederà se l'utente intende salvare quell'elenco per utilizzarlo successivamente quando si

ripirstinano le impostazioni iniziali. Per salvare l'elenco degli oggetti, selezionare **Ambito protezione** nella finestra **Impostazioni**: **File Anti-Virus** che si apre.

7.2.6. Selezione delle azioni da applicare agli oggetti

Se durante la scansione antivirus File Anti-Virus rileva o sospetta la presenza di un'infezione all'interno di un file, le fasi successive dipendono dallo stato dell'oggetto e dall'azione selezionata.

File Anti-Virus applica agli oggetti i seguenti stati:

- Programma nocivo (per esempio, *virus, trojan)*.
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il programma ha rilevato una sequenza di codice nel file proveniente da un virus sconosciuto o un codice modificato di un virus noto.

Per impostazione predefinita, tutti i file infetti sono sottoposti a un tentativo di riparazione e se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

Aprire la finestra delle impostazioni dell'applicazione e selezionare **File Anti-Virus** sotto **Impostazioni**. Tutte le azioni potenziali sono visualizzate nelle sezioni appropriate (vedi Figura 24).

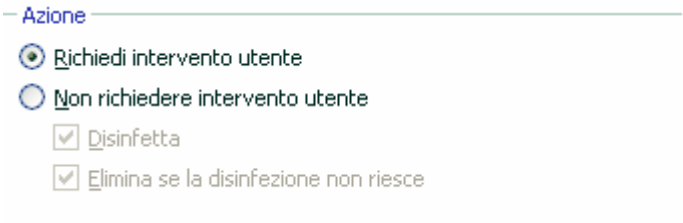


Figura 24. Azioni possibili di File Anti-Virus in caso di oggetti pericolosi

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
Richiedi intervento utente	File Anti-Virus visualizza un avvertimento contenente informazioni sul programma nocivo che ha o potrebbe aver infettato il file e propone una serie di azioni da scegliere. Tali azioni dipendono dallo stato dell'oggetto.

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
Non richiedere intervento utente	File Anti-Virus blocca l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report (vedi 19.3 a pag. 269). In un secondo momento sarà possibile tentare di disinfettare l'oggetto.
Non richiedere intervento utente **Disinfetta**	File Anti-Virus blocca l'accesso all'oggetto e cerca di disinfettarlo. Se la riparazione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non è stata possibile, l'oggetto viene spostato in Quarantena (vedi 19.1 a pag. 263). Le informazioni relative all'evento vengono registrate nel report. In un secondo momento sarà possibile tentare di disinfettare l'oggetto.
Non richiedere intervento utente **Disinfetta** **Elimina se la disinfezione non riesce**	File Anti-Virus blocca l'accesso all'oggetto e cerca di disinfettarlo. Se la disinfezione ha esito positivo, il file viene ripristinato per l'uso. Se la disinfezione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene conservata nel Backup (vedi 19.2 a pag. 266).
Non richiedere intervento utente **Disinfetta** **Elimina**	File Anti-Virus blocca l'accesso all'oggetto e lo elimina.

Quando disinfetta o elimina un oggetto, Kaspersky Internet Security crea una copia di backup prima di tentare di riparare l'oggetto o di eliminarlo, per poter ripristinare l'oggetto in seguito o nel caso emerga la possibilità di ripararlo.

7.3. Disinfezione posticipata

Se l'azione da applicare ai programmi nocivi è **Non richiedere intervento utente**, l'accesso agli oggetti viene bloccato e la disinfezione non viene eseguita.

Se l'azione selezionata fosse

Non richiedere intervento utente

Disinfetta

sarebbe bloccato l'accesso anche a tutti gli oggetti non trattati.

Per poter accedere di nuovo agli oggetti bloccati è necessario prima ripararli. Procedere come segue:

1. Selezionare **File Anti-Virus** sotto **Protezione** nella finestra principale del programma e fare clic su Apri report.
2. Selezionare gli oggetti desiderati nella scheda **Rilevato** e fare clic sul pulsante **Azioni → Disinfetta tutto**.

Se riparato con successo, l'oggetto sarà messo di nuovo a disposizione dell'utente. Se la riparazione non riesce, è possibile *eliminare* l'oggetto o *ignorarlo*. In quest'ultimo caso, l'accesso al file sarà ripristinato. Questo tuttavia incrementa considerevolmente il rischio di infezione del computer, pertanto si raccomanda di non ignorare gli oggetti nocivi.

CAPITOLO 8. MAIL ANTI-VIRUS

Kaspersky Internet Security comprende uno speciale componente che protegge la posta in arrivo e in uscita dagli oggetti pericolosi: *Mail Anti-Virus*. Esso viene eseguito all'avvio del sistema, rimane attivo nella memoria di sistema ed esamina tutta la posta basata sui protocolli POP3, SMTP, IMAP, MAPI[1] e NNTP, ed anche le connessioni protette (SSL) che utilizzano POP3 e IMAP.

L'indicatore di funzionamento del componente è l'icona nell'area di notifica della barra delle applicazioni di Kaspersky Internet Security, che durante la scansione di un messaggio di posta elettronica assume questo aspetto  .

La configurazione predefinita di Mail Anti-Virus è la seguente:

1. Mail Anti-Virus intercetta ciascun messaggio ricevuto o inviato dall'utente.
2. Il messaggio viene suddiviso nelle parti che lo compongono: intestazione, corpo del messaggio, allegati.
3. Il corpo del messaggio e gli allegati (inclusi gli allegati OLE) vengono esaminati per escludere la presenza di oggetti pericolosi. Gli oggetti nocivi vengono individuati per mezzo dei database inclusi nel programma e con l'algoritmo euristico. I database contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.
4. Dopo la scansione antivirus è possibile scegliere tra le seguenti azioni:
    - Se il corpo del messaggio o gli allegati contengono codici nocivi, Mail Anti-Virus blocca il messaggio, salva una copia dell'oggetto infetto nella cartella *Backup* e cerca di riparare l'oggetto. Se la riparazione del messaggio ha esito positivo, esso viene reso nuovamente disponibile per l'utente. In caso contrario, l'oggetto infetto all'interno del messaggio viene eliminato. Dopo la scansione antivirus, nel campo dell'oggetto del messaggio viene inserito un testo che dichiara che il messaggio è stato esaminato da Kaspersky Internet Security.

[1] Le e-mail inviate con MAPI sono scansionate utilizzando uno speciale plug-in per Microsoft Office Outlook e The Bat!

- Se nel corpo del messaggio o in un allegato viene individuato un codice che sembra nocivo ma senza alcuna certezza, la parte sospetta del messaggio viene trasferita nella cartella *Quarantena*.
- Se all'interno del messaggio non viene individuato alcun codice nocivo, il messaggio viene reso nuovamente disponibile.

Il programma è dotato di uno speciale plug-in (vedi 8.2.2 a pag. 114) per MS Outlook in grado di configurare le scansioni della posta con maggior precisione.

Se il client di posta utilizzato è The Bat!, è possibile usare Kaspersky Internet Security in aggiunta ad altre applicazioni antivirus. Le regole di trattamento del traffico e-mail (vedi 8.2.3 a pag. 116) sono configurate direttamente in The Bat! e sostituiscono le impostazioni di protezione della posta di Kaspersky Internet Security.

Quando si lavora con altri programmi di posta (fra cui Outlook Express, Mozilla Thunderbird, Eudora, Incredimail), Mail Anti-Virus esamina la posta basata sui protocolli SMTP, POP3, IMAP, MAPI e NNTP.

Attenzione!

Osservare che i messaggi trasmessi mediante il protocollo IMAP non vengono esaminati in Thunderbird se si fa uso di filtri che li trasferiscono fuori dalla casella di posta in **Arrivo**.

8.1. Selezione di un livello di sicurezza della posta elettronica

Kaspersky Internet Security protegge la posta elettronica in base a uno dei seguenti livelli (vedi Figura 25):

Protezione massima – il livello che garantisce il monitoraggio più approfondito della posta in entrata e in uscita. Il programma esamina approfonditamente gli allegati di posta, inclusi gli archivi, indipendentemente dalla durata della scansione.

Consigliato. È il livello consigliato dagli esperti Kaspersky Lab. A questo livello di protezione vengono esaminati gli stessi oggetti del livello **Protezione massima**, con l'eccezione degli allegati o dei messaggi la cui scansione richiederebbe più di 3 minuti.

Alta velocità – livello di sicurezza le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla limitazione dell'ambito della scansione. In base a queste impostazioni, viene esaminata solo la posta in entrata, escludendo però gli archivi e gli oggetti (e-mail) allegati la cui scansione richiederebbe più di tre

minuti. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione della posta elettronica.

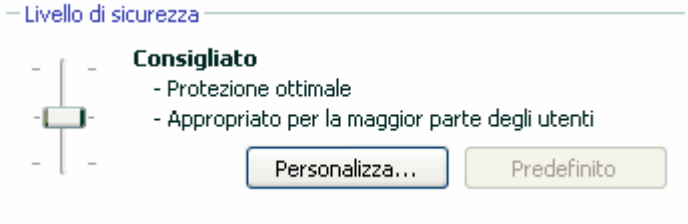


Figura 25. Selezione di un livello di protezione della posta elettronica

Per impostazione predefinita, la protezione della posta elettronica è impostata su **Consigliato**.

È possibile aumentare o ridurre il livello di protezione della posta selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Modificando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di oggetti esaminati: La velocità di scansione è inversamente proporzionale al numero di oggetti e-mail esaminati.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile personalizzarli. E' consigliabile selezionare un livello il più vicino possibile alle proprie necessità, poi modificarne i parametri. Questo modificherà il nome del livello di sicurezza in **Personalizzato.** Ecco un esempio in cui potrebbe essere necessario modificare le impostazioni preconfigurate dei livelli di sicurezza.

Esempio:

Il computer si trova all'esterno della LAN e si connette a Internet mediante connessione remota. Il client installato per ricevere e inviare la posta elettronica è Outlook Express e il servizio utilizzato è gratuito. Per varie ragioni, il traffico di posta elettronica prevede un certo numero di archivi allegati. Come garantire una protezione ottimale del computer dalle infezioni trasmesse attraverso la posta elettronica?

Suggerimento per selezionare un livello:

Analizzando la situazione, si potrebbe concludere che il rischio di infezione attraverso la posta elettronica sia piuttosto elevato a causa dell'assenza di una protezione centralizzata della posta elettronica e del metodo di connessione a Internet).

Il livello di protezione consigliato è quindi **Protezione massima**, al quale apportare le seguenti modifiche: Si consiglia di ridurre il tempo di scansione

degli allegati, per esempio a 1-2 minuti. La maggior parte degli archivi allegati sarà così sottoposta a scansione antivirus ma la velocità di elaborazione non sarà pregiudicata.

Per modificare il livello di protezione attuale:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Mail Anti-Virus** in **Protezione**.
2. Fare clic su **Personalizza** in **Livello di sicurezza** (vedi Figura 25).
3. Impostare i parametri di protezione della posta nella finestra e fare clic su **OK**.

8.2. Configurazione di Mail Anti-Virus

Le modalità di scansione della posta dipendono da una serie di impostazioni che possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono il gruppo di messaggi protetto (vedi 8.2.1 a pag. 112).
- Impostazioni che definiscono l'utilizzo di metodi euristici (vedi Sezione 8.2.4 a pag. 118).
- Impostazioni di scansione della posta per MS Outlook (vedi 8.2.2 a pag. 114) e The Bat! (vedi 8.2.3 a pag. 116).
- Impostazioni che definiscono le azioni da eseguire in caso di oggetti di posta pericolosi (vedi 8.2.5 a pag. 119).

La presente sezione prende in esame queste impostazioni.

8.2.1. Selezione di un gruppo di messaggi protetto

Mail Anti-Virus consente di selezionare i gruppi di messaggi da esaminare per escludere la presenza di oggetti pericolosi.

Per impostazione predefinita, il componente protegge la posta elettronica al livello di protezione **Consigliato**, esaminando cioè sia i messaggi in arrivo sia quelli in uscita. La prima volta che si lavora con il programma è consigliabile esaminare la posta in uscita in quanto è probabile che il computer nasconda worm che si servono della posta elettronica come canale di diffusione. Questo accorgimento eviterà il rischio che il computer invii inavvertitamente mailing di massa con oggetti infetti.

Se si è certi che i messaggi che si inviano non contengano oggetti pericolosi, è possibile disabilitare la scansione della posta in uscita procedendo come segue:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Mail Anti-Virus** in **Protezione**.
2. Fare clic sul pulsante **Personalizza** nell'area **Livello di sicurezza** (vedi Figura 25).
3. Nella finestra che si apre (vedi Figura 26), selezionare **Solo posta in entrata** nella sezione **Ambito**.

Oltre a selezionare un gruppo di messaggi, è possibile specificare se sottoporre alla scansione anche gli archivi allegati e impostare la durata massima della scansione di un oggetto di posta. Queste impostazioni vengono configurate nella sezione **Restrizioni**.

Se il computer non è protetto da alcun software di rete locale e la connessione a Internet non prevede l'uso di un server proxy o di una firewall, si raccomanda di non disabilitare la scansione degli archivi allegati e di non impostare una limitazione temporale alla scansione.

Se invece si lavora in un ambiente protetto, è possibile modificare le limitazioni temporali alla scansione in modo da incrementare la velocità.

Figura 26. Impostazioni di Mail Anti-Virus

È possibile configurare anche le condizioni di filtro degli oggetti allegati a un messaggio nella sezione **Filtro allegati**:

- **Disattiva filtro** – consente di non utilizzare ulteriori filtri per gli allegati.
- **Rinomina tipi di allegati selezionati** – consente di escludere gli allegati di formati specifici e di sostituire l'ultimo carattere del nome di un file con un trattino di sottolineatura. Per selezionare il tipo di file, fare clic sul pulsante **Tipi di file...**.
- **Elimina tipi di allegati selezionati** – consente di escludere ed eliminare gli allegati di formati specifici. Per selezionare il tipo di file, fare clic sul pulsante **Tipi di file**.

Per ulteriori informazioni sui tipi di allegati filtrati consultare la sezione A.1 a pag. 334.

L'uso del filtro rappresenta un'ulteriore sicurezza per il computer, poiché nella maggior parte dei casi i programmi nocivi si diffondono attraverso la posta in forma di allegati. Rinominando o eliminando determinati tipi di allegati, si previene l'apertura automatica degli allegati all'arrivo di un messaggio.

8.2.2. Configurazione del trattamento della posta in Microsoft Office Outlook

Se il client di posta utilizzato è Microsoft Office Outlook, è possibile impostare una configurazione personalizzata delle scansioni antivirus.

Durante l'installazione di Kaspersky Internet Security, viene installato in Outlook uno speciale plug-in in grado di accedere rapidamente alle impostazioni di Mail Anti-Virus e di impostare l'ora di avvio massima della scansione antivirus dei messaggi.

Il plug-in ha l'aspetto di una scheda di **Mail Anti-Virus** ubicata in **Strumenti** → **Impostazioni** (vedi Figura 27).

Selezionare una modalità di scansione della posta:

- **Scansiona alla ricezione** – consente di analizzare ogni messaggio nel momento in cui viene consegnato.
- **Scansiona alla lettura** – consente di esaminare i messaggi nel momento in cui vengono aperti.
- **Scansiona all'invio** – consente di eseguire la scansione antivirus dei messaggi in uscita nel momento dell'invio.

Attenzione!

Se si utilizza Outlook per connettersi al server di posta mediante protocollo IMAP, si raccomanda di non utilizzare la modalità **Scansiona alla ricezione**. Se si abilita questa modalità, i messaggi di posta elettronica vengono copiati sul computer locale alla consegna al server, perdendo di conseguenza il vantaggio principale del protocollo IMAP, cioè la riduzione del traffico e la gestione della posta indesiderata direttamente sul server senza copiarla sul computer dell'utente.

L'azione da eseguire sugli oggetti di posta pericolosi è definita tra le impostazioni di Mail Anti-Virus. Per configurarle, seguire il link cliccare qui nella sezione **Stato**.

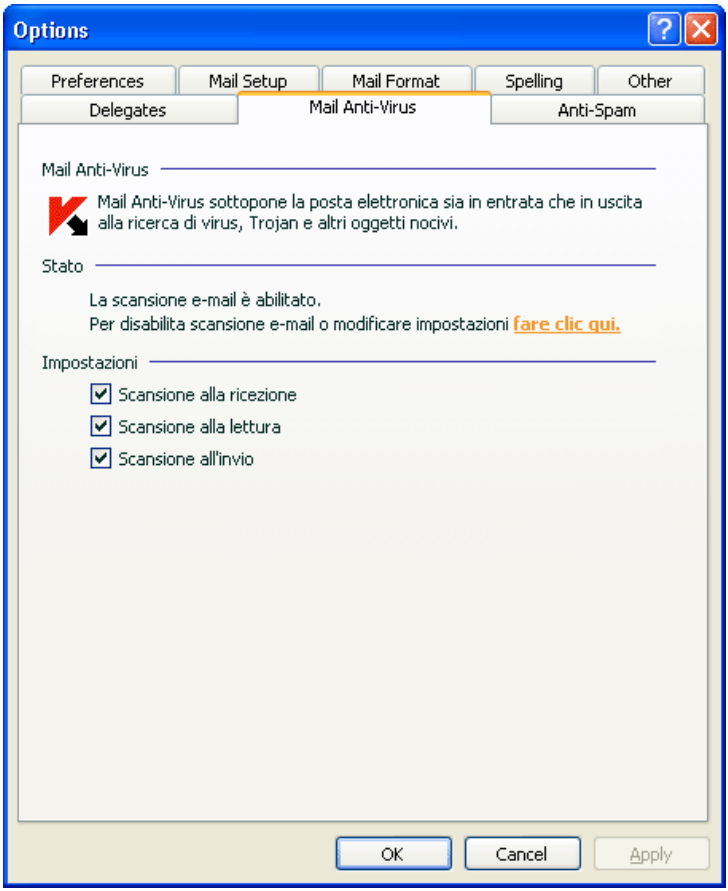


Figura 27. Configurazione delle impostazioni di Mail Anti-Virus in MS Outlook

8.2.3. Configurazione delle scansioni di posta in The Bat!

Le azioni da eseguire sugli oggetti di posta infetti in The Bat! sono definite per mezzo degli strumenti del programma.

Attenzione!

Le impostazioni di Mail Anti-Virus che determinano se esaminare i messaggi in arrivo e in uscita, nonché le azioni da eseguire sugli oggetti di posta pericolosi e le esclusioni, sono ignorate. Gli unici elementi di cui The Bat! tiene conto sono la scansione degli archivi allegati e le limitazioni temporali della scansione dei messaggi (vedi 8.2.1 a pag. 112).

Per impostare le regole di protezione della posta in The Bat!:

1. Selezionare **Impostazioni** dal menu **Proprietà** del programma di posta.
2. Selezionare **Protezione virus** dalla struttura ad albero delle impostazioni.

Le impostazioni di protezione visualizzate (vedi Figura 28) valgono per tutti i moduli antivirus installati nel computer che supportano The Bat!

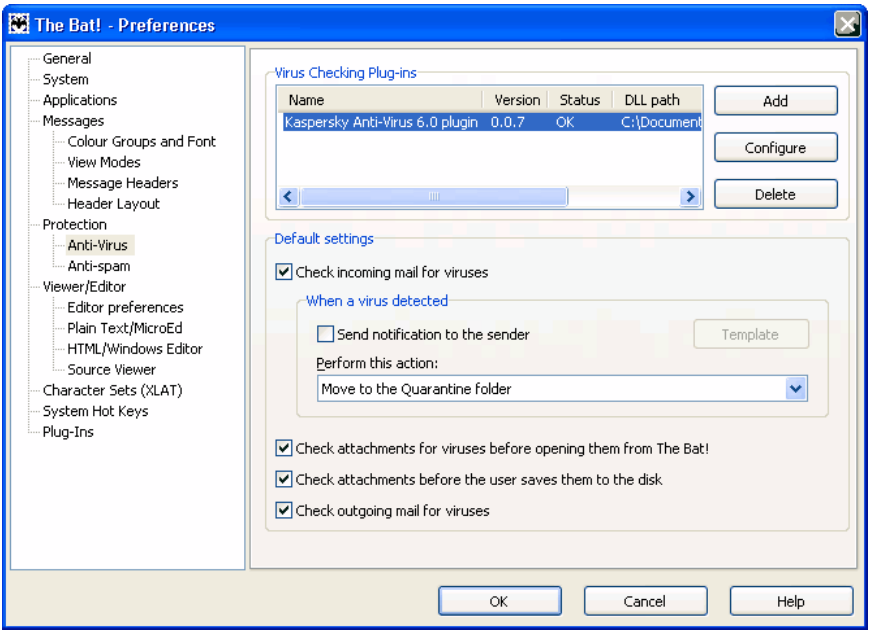


Figura 28. Configurazione delle scansioni di posta in The Bat!

A questo punto occorre stabilire:

- Quali gruppi di messaggi saranno sottoposti alla scansione antivirus (in arrivo, in uscita).
- In quale momento gli oggetti di posta saranno sottoposti alla scansione antivirus (all'apertura del messaggio o prima di salvarlo sul disco).
- Le azioni da eseguire in caso di intercettazione di oggetti pericolosi nei messaggi. Per esempio, è possibile selezionare:

  Prova a curare le parti infettate – consente di riparare l'oggetto di posta infetto; se la riparazione non riesce, l'oggetto resta nel messaggio. Kaspersky Internet Security informa sempre l'utente ogni volta che viene individuato un messaggio infetto. Ma anche selezionando **Elimina** nella finestra degli avvisi di Mail Anti-Virus, l'oggetto rimane nel messaggio poiché l'azione selezionata in The Bat! ha la precedenza su quelle di Mail Anti-Virus.

  Rimuovi le parti infettate – consente di eliminare l'oggetto pericoloso dal messaggio, sia esso effettivamente infetto o solo sospettato di esserlo.

Per impostazione predefinita, The Bat! trasferisce tutti gli oggetti di posta infetti nella cartella Quarantena senza ripararli.

Attenzione!

The Bat! non evidenzia con intestazioni speciali i messaggi contenenti oggetti pericolosi.

8.2.4. Utilizzo dell'analisi euristica

I metodi euristici sono utilizzati da diversi componenti di protezione in tempo reale e da metodi di scansione virus (vedi sezione 7.2.4 a pag. 103 per maggiori dettagli).

I metodi euristici per l'individuazione di nuove minacce possono venire abilitati/disabilitati per i componenti di Mail Anti-Virus utilizzando la scheda **Analizzatore Euristico**. Per questo è necessario eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Mail Anti-Virus** in **Protezione**.
2. Fare clic sul pulsante **Personalizza** nell'area **Livello di sicurezza** (vedi Figura 25).
3. Selezionare la scheda **Analizzatore Euristico** nella finestra di dialogo che compare (vedi Figura 29).

Per utilizzare i metodi euristici, selezionare **Usa analizzatore euristico**. Inoltre, la risoluzione della scansione può essere impostata spostando il cursore su una delle seguenti impostazioni: **basso, medio o dettagliato**.

Figura 29. Utilizzo dell'analisi euristica

8.2.5. Ripristino delle impostazioni predefinite di Mail Anti-Virus

Durante la configurazione di Mail Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni predefinite di Mail Anti-Virus:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Mail Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza** (vedi Figura 25).

8.2.6. Selezione delle azioni da eseguire sugli oggetti di posta pericolosi

Se una scansione della posta evidenzia messaggi o parti di messaggio (intestazione, corpo, allegati) infetti o sospetti, le operazioni successive di Mail Anti-Virus dipendono dallo stato dell'oggetto e dall'azione selezionata.

Dopo la scansione, agli oggetti di posta possono essere associati i seguenti stati:

- Stato di programma nocivo (per esempio, virus, trojan, per ulteriori informazioni, vedi 1.1 a pag. 11).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il codice del file contiene una sezione che sembra essere la variante di un virus noto o ricorda la struttura di una sequenza virale.

Per impostazione predefinita, quando Mail Anti-Virus rileva un oggetto pericoloso o potenzialmente infetto, visualizza un avviso e invita l'utente di selezionare un'azione.

Per modificare un'azione da applicare a un oggetto:

Aprire la finestra delle impostazioni di Kaspersky Internet Security e selezionare **Mail Anti-Virus** sotto **Protezione**. Tutte le azioni possibili per gli oggetti pericolosi sono elencate nella casella **Azione** (vedi Figura 30).

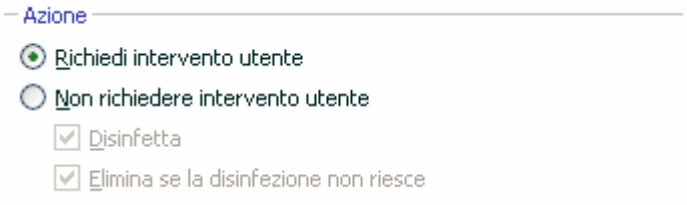


Figura 30. Selezione delle azioni da eseguire sugli oggetti di posta pericolosi

Osserviamo adesso in dettaglio le possibili opzioni di trattamento degli oggetti di posta pericolosi.

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
Richiedi intervento utente	Mail Anti-Virus visualizza un avviso con informazioni sul programma nocivo che ha infettato (o potenzialmente infettato) il file e offre l'opzione di una delle seguenti azioni.
Non richiedere intervento utente	Mail Anti-Virus blocca l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report (vedi 19.3 a pag. 269). In un secondo momento sarà possibile tentare di riparare l'oggetto.
Non richiedere intervento utente **Disinfetta**	Mail Antivirus bloccherà l'accesso all'oggetto e tenterà di disinfettarlo. Se viene disinfettato con successo, verrà poi ripristinato per un utilizzo regolare. Se invece il programma non riesce a riparare l'oggetto, questo viene messo in Quarantena (vedi 19.1.1 a pag. 264). Le informazioni su di esso vengono registrate nel report. Più tardi sarà possibile tentare di disinfettare l'oggetto.
Non richiedere intervento utente **Disinfetta** **Elimina se la disinfezione non riesce**[2]	Mail Anti-Virus bloccherà l'accesso all'oggetto e tenterà di disinfettarlo. Se viene disinfettato con successo, verrà poi ripristinato per un utilizzo regolare. Se l'oggetto non può essere disinfettato, viene eliminato. Una copia dell'oggetto viene archiviata nel Backup. Gli oggetti potenzialmente infetti verranno messi in Quarantena.
Non richiedere intervento utente **Elimina**	Quando Mail Anti-Virus individua un oggetto infetto o potenzialmente infetto, lo elimina senza informare l'utente.

[2] Se il client in uso è The Bat!, gli oggetti di posta pericolosi vengono riparati o eliminati quando Mail Anti-Virus esegue questa azione (a seconda dell'azione selezionata in The Bat!).

Quando disinfetta od elimina un oggetto, Kaspersky Internet Security crea una copia di backup e la invia nella cartella Backup (vedi 19.2 a pag. 267) da dove potrà essere recuperato qualora si renda necessario il ripristino dell'oggetto o si presenti un'opportunità di ripararlo.

CAPITOLO 9. WEB ANTI-VIRUS

Ogni volta che si usa Internet, si espongono le informazioni custodite nel computer al rischio di infezione da parte di programmi pericolosi. Questi possono essere caricati nel computer aprendo un determinato sito web o leggendo un articolo su Internet.

Kaspersky Internet Security include uno speciale componente per la protezione del computer durante la navigazione su Internet: *Web Anti-Virus*. Esso protegge le informazioni che entrano nel computer attraverso il protocollo HTTP e impedisce il caricamento di script pericolosi sul computer.

Attenzione!

Web Anti-Virus controlla solo il traffico HTTP che passa attraverso le porte elencate nell'elenco delle porte monitorate (vedi 19.5 pag. 291). Il pacchetto del programma include un elenco delle porte più comunemente utilizzate per la trasmissione della posta e del traffico HTTP. Se si utilizzano porte non presenti in questo elenco è necessario aggiungerle al fine di proteggere il traffico che passa attraverso di esse.

Se si lavora su una rete non protetta si raccomanda di utilizzare Web Anti-Virus per proteggere il computer durante l'uso di Internet. Se il computer è collegato a una rete protetta da firewall o da filtri per il traffico HTTP, Web Anti-Virus offre un'ulteriore protezione durante la navigazione sul Web.

L'indicatore di funzionamento del componente è l'icona nell'area di notifica della barra delle applicazioni di Kaspersky Internet Security, che durante la scansione di uno script assume questo aspetto  .

Osserviamo in dettaglio il funzionamento del componente.

Web Anti-Virus si compone di due moduli che gestiscono:

- *Scansione traffico* – scansione degli oggetti che entrano nel computer mediante HTTP.
- *Scansione script* – scansione di tutti gli script elaborati in Microsoft Internet Explorer come pure gli script WSH (JavaScript, Visual Basic Script, ecc.) caricati durante l'uso del computer.

  È presente inoltre uno speciale plug-in per Microsoft Internet Explorer che viene installato con Kaspersky Internet Security. L'icona  nella barra dei degli strumenti standard del browser significa che esso è installato. Facendo clic sull'icona, si apre una finestra contenente le statistiche di Web Anti-Virus sul numero di script esaminati e bloccati.

Web Anti-Virus monitora il traffico HTTP con le seguenti modalità:

1. Ogni pagina web o file accessibile all'utente o a un determinato programma via HTTP viene intercettata e analizzata da Web Anti-Virus per escludere la presenza di codici nocivi. Gli oggetti nocivi vengono individuati sia attraverso i database di Kaspersky Internet Security che attraverso l'algoritmo euristico. I database contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nei database.
2. Dopo l'analisi è possibile agire come segue:
   - Se una pagina web o un oggetto a cui l'utente sta cercando di accedere contengono un codice nocivo, l'accesso ad essi viene bloccato. Viene quindi visualizzato un messaggio che informa che l'oggetto o la pagina è infetta.
   - Se il file o la pagina web non contengono codici nocivi, essa è immediatamente accessibile all'utente.

Gli script vengono esaminati secondo il seguente algoritmo:

1. Web Anti-Virus intercetta ogni script eseguito in una pagina web e lo esamina per escludere la presenza di codici nocivi.
2. Se uno script contiene un codice nocivo, Web Anti-Virus lo blocca e informa l'utente con uno speciale pop-up.
3. Se nello script non viene rilevato alcun codice nocivo, esso viene eseguito.

Attenzione!

Al fine di intercettare e sottoporre il traffico http e gli script a scansione anti-virus, Web Anti-Virus deve essere già in funzione prima di collegarsi a una risorsa web. In caso contrario, il traffico non sarà analizzato.

9.1. Selezione del livello di protezione web

Kaspersky Internet Security protegge il computer durante la navigazione in Internet in base a uno dei seguenti livelli (vedi Figura 31):

Protezione massima – il livello che garantisce il monitoraggio più approfondito di script e oggetti in entrata via HTTP. Il programma esegue un'accurata scansione di tutti gli oggetti utilizzando l'intero set di

database dell'applicazione. Questo livello di sicurezza è consigliato per gli ambienti aggressivi in cui non si utilizzano altri strumenti di protezione per gli HTTP.

Consigliato. È il livello consigliato dagli esperti Kaspersky Lab. Questo livello esamina gli stessi oggetti del livello **Protezione massima**, ma limita il tempo di cache dei frammenti di file, accelerando così la scansione e rendendo disponibili gli oggetti più rapidamente.

Alta velocità – è un livello di protezione le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla restrizione dell'ambito della scansione ottenuta utilizzando un numero di database dell'applicazione limitato. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione web.

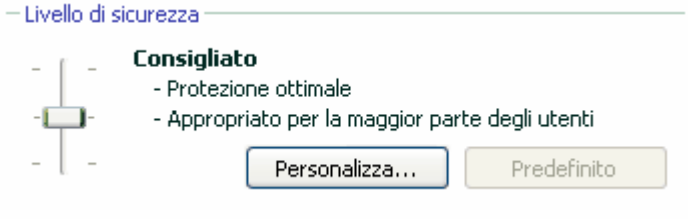


Figura 31. Selezione di un livello di protezione web

Per impostazione predefinita, la protezione è impostata sul livello **Consigliato**.

È possibile aumentare o ridurre il livello di sicurezza selezionando quello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Modificando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di oggetti esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di oggetti esaminati.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile crearne uno personalizzato. Raccomandiamo di selezionare il livello il più vicino alle proprie necessità e di modificarne i parametri. Il nome del livello di sicurezza verrà cambiato in Personalizzato. Osserviamo un esempio in cui è utile modificare le impostazioni predefinite del livello di sicurezza.

Esempio:

Il computer dell'utente si connette a Internet via modem. Non è connesso a una LAN aziendale e non è protetto da alcuna misura antivirus per il traffico HTTP in entrata.

A causa della natura stessa del proprio lavoro, l'utente scarica regolarmente file di grandi dimensioni da Internet. La scansione di file di questo genere, di norma, richiede tempi piuttosto lunghi.

Occorre pertanto garantire un'ottimale protezione del computer contro le infezioni trasmesse con il traffico HTTP o gli script.

Suggerimento per selezionare un livello:

Da queste informazioni basilari, possiamo concludere che il computer lavora in un ambiente sensibile e che il rischio di contrarre infezioni attraverso il traffico HTTP è elevato (nessuna protezione web centralizzata, metodo di connessione a Internet dial-up).

Il livello di protezione consigliato è quindi **Protezione massima**, apportando le seguenti modifiche: Si raccomanda di ridurre il tempo di cache dei frammenti di file durante la scansione.

Per modificare un livello di sicurezza predefinito:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Web Anti-Virus** sotto **Protezione**.
2. Cliccare su **Personalizza…** sotto **Livello di sicurezza** (vedi Figura 31).
3. Modificare i parametri di protezione del browser nella risultante finestra e cliccare su **OK**.

9.2. Configurazione di Web Anti-Virus

Web Anti-Virus esamina tutti gli oggetti caricati nel computer attraverso il protocollo HTTP e monitora tutti gli script WSH (script JavaScript, Visual Basic ecc.) che vengono eseguiti.

È possibile configurare le impostazioni di Web Anti-Virus in modo da accelerare la velocità di funzionamento del componente, in particolare:

- Configurazione delle impostazioni generali di scansione (vedi 9.2.1 a pag. 127).
- Creazione di un elenco di indirizzi web attendibili (vedi 9.2.2 pag. 128).
- Abilitazione/disabilitazione dell'analisi euristica (vedi 9.2.3 pag. 129).

Inoltre è possibile selezionare le azioni che Web Anti-Virus eseguirà ogni volta che rileva oggetti HTTP pericolosi.

La presente sezione prende in esame queste impostazioni.

9.2.1. Impostazioni generali di scansione

Per aumentare il tasso di successo nel rilevamento dei codici nocivi, Web Anti-Virus ripone nella cache i frammenti degli oggetti scaricati da Internet. Con questo metodo, Web Anti-Virus scansiona un oggetto solo dopo averlo scaricato completamente. A quel punto, l'oggetto è sottoposto a scansione anti-virus e, in base al risultato, il programma rende l'oggetto disponibile all'utente o lo blocca.

Tuttavia, l'utilizzo dell'area cache aumenta il tempo di elaborazione dell'oggetto e il tempo entro il quale il programma lo restituisce all'utente, e può inoltre causare problemi al momento della copia e dell'elaborazione di oggetti pesanti a causa del timeout della connessione con l'http client.

Per risolvere questo problema, si consiglia di limitare il tempo di cache per i frammenti di oggetti web scaricati da Internet. Allo scadere di questo intervallo di tempo, l'utente riceverà la parte scaricata del file non scansionata e, al completamento del download dell'oggetto, questo sarà scansionato nella sua interezza. In questo modo, l'oggetto è disponibile all'utente entro minor tempo e si risolve il problema di interruzione della connessione, senza tuttavia ridurre il livello di sicurezza durante l'uso di Internet.

Per impostazione predefinita, il tempo di cache per i frammenti di file è limitato a un secondo. Aumentando questo valore o deselezionando il limite del tempo di cache i risultati di scansione migliorano, ma in una certa misura rallentano i tempi di consegna dell'oggetto.

Per limitare il tempo di cache per i frammenti di file o rimuovere il limite:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Web Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Personalizza** nell'area **Livello di sicurezza** (vedi Figura 31).
3. Nella finestra che si apre (vedi Figura 32), selezionare l'opzione desiderata nella sezione **Impostazioni di scansione**.

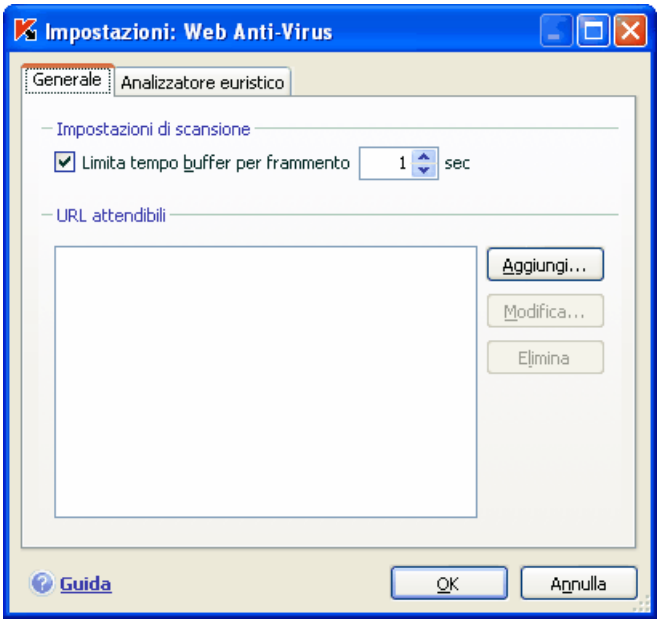


Figura 32. Selezione del livello di protezione web

9.2.2. Creazione di un elenco di indirizzi attendibili

È possibile creare un elenco di indirizzi i cui contenuti sono ritenuti attendibili. Web Anti-Virus non analizzerà i dati provenienti da quegli indirizzi. Questa opzione può essere utilizzata nei casi in cui Web Anti-Virus blocca ripetutamente un particolare file ogni volta che si tenta di scaricarlo.

Per creare un elenco degli indirizzi attendibili:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Web Anti-Virus** sotto **Protezione**.
2. Cliccare sul pulsante **Personalizza…** sotto **Livello di sicurezza** (vedi Figura 31).
3. Nella finestra che si apre (vedi Figura 32), creare un elenco dei server attendibili nella sezione **URL attendibili**. A questo scopo utilizzare i pulsanti sulla destra dell'elenco.

Al momento di digitare un indirizzo affidabile, è possibile creare delle maschere con i seguenti caratteri jolly:

*– qualsiasi combinazione di caratteri.

Esempio: Se si è creata la maschera ***abc***, non verrà esaminato alcun URL contenente la sequenza **abc**. Ad esempio: www.virus.com/download_virus/page_0-9abcdef.html

? – qualsiasi carattere singolo.

Esempio: Se si è creata la maschera **Patch_123?.com**, gli URL contenenti quella serie di caratteri più qualsiasi carattere singolo dopo il 3 non saranno esaminati. Ad esempio: **Patch_1234.com.** Tuttavia l'URL **patch_12355.com** sarà esaminato.

Se i caratteri * o ? fanno effettivamente parte dell'URL da aggiungere all'elenco, digitare una barra rovesciata per escludere il carattere * o ? che segue.

Esempio: Si desidera aggiungere questo URL all'elenco degli indirizzi attendibili: www.virus.com/download_virus/virus.dll?virus_name=

Per evitare che Kaspersky Internet Security consideri il **?** come un carattere jolly, è necessario farlo precedere da una barra rovesciata (\ ). Così facendo, l'URL aggiunto all'elenco delle esclusioni sarà come segue: www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Utilizzo dell'analisi euristica

I metodo euristici vengono utilizzati da numerosi componenti di protezione in tempo reale e attività di scansione anti-virus (vedi 7.2.4 pag. 103 per maggiori dettagli).

I metodi euristici di riconoscimento di nuove minacce possono essere abilitati/disabilitati per il componente Web Anti-Virus utilizzando la scheda **Analizzatore Euristico**. Occorre seguire i seguenti passaggi:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Web Anti-Virus** sotto **Protezione**.
2. Cliccare sul pulsante **Personalizza...** nell'area **Livello di sicurezza**.
3. Selezionare la scheda **Analizzatore Euristico** nella finestra di dialogo che si apre (vedi Figura 33).

Per utilizzare il metodo euristico spuntare ☑ **Usa Analizzatore Euristico.** Inoltre la risoluzione della scansione può essere selezionata muovendo il cursore su una delle seguenti opzioni: **Basso, Medio, Dettagliato**.

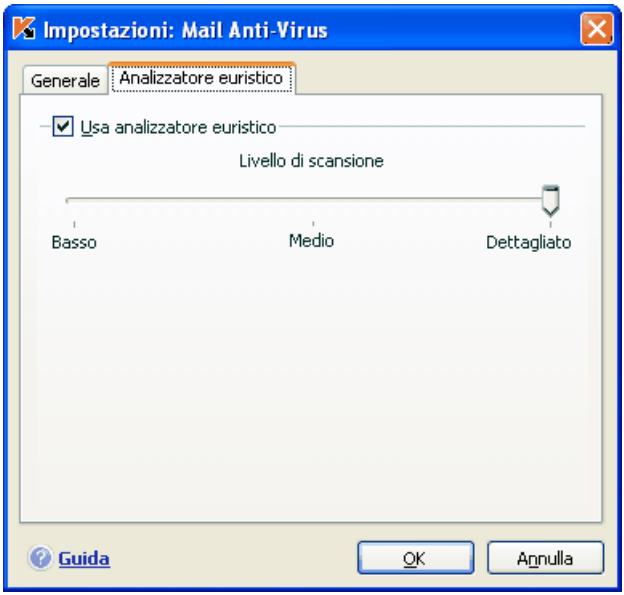


Figura 33. Utilizzo dell'analisi euristica

9.2.4. Ripristino delle impostazioni predefinite di Web Anti-Virus

Durante la configurazione di Web Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni predefinite che Kaspersky Lab considera ottimali e che ha riunito nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni predefinite di Web Anti-Virus:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Web Anti-Virus** sotto **Protezione**.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza** (vedi Figura 31).

9.2.5. Selezione delle reazioni agli oggetti pericolosi

Se l'analisi di un oggetto HTTP evidenzia la presenza di un codice nocivo, la reazione di Web Anti-Virus dipende dall'azione selezionata dall'utente.

Per configurare le reazioni di Web Anti-Virus in presenza di un oggetto pericoloso:

Aprire la finestra delle impostazioni dell'applicazione e selezionare il componente **Web Anti-Virus** sotto **Protezione**. Tutte le azioni possibili per gli oggetti pericolosi sono elencate nella sezione **Azione** (vedi Figura 34).

Per impostazione predefinita, in presenza di un oggetto HTTP pericoloso Web Anti-Virus visualizza un avviso e propone una scelta di azioni da eseguire sull'oggetto.

Figura 34. Selezione di azioni da eseguire su script pericolosi

Le possibili opzioni di trattamento degli oggetti HTTP pericolosi sono le seguenti:

Se l'azione selezionata era	**Se viene intercettato un oggetto pericoloso nel traffico HTTP**
Richiedi intervento utente	Web Anti-Virus visualizza un avviso contenente informazioni sul codice nocivo che potrebbe aver infettato l'oggetto e offre una serie di opzioni.
Blocca	Web Anti-Virus blocca l'accesso all'oggetto e visualizza un avviso in merito. Le informazioni relative all'evento vengono registrate nel report (vedi 19.3 a pag. 269).
Consenti	Web Anti-Virus consente l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report.

Per quanto riguarda gli script pericolosi, Web Anti-Virus li blocca sempre e visualizza messaggi che avvisano l'utente dell'azione eseguita. Non è possibile modificare la reazione a uno script pericoloso; l'unica alternativa consiste nel disabilitare il modulo di scansione degli script.

CAPITOLO 10. DIFESA PROATTIVA

Attenzione!

In questa versione dell'applicazione non c'è il componente **Controllo Integrità Applicazione** sui computer con sistema operativo Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64.

Kaspersky internet Security protegge sia dalle minacce note sia da quelle sulle quali non si possiedono ancora informazioni nei database dell'applicazione. Questa protezione è garantita da un componente appositamente sviluppato, *Difesa proattiva.*

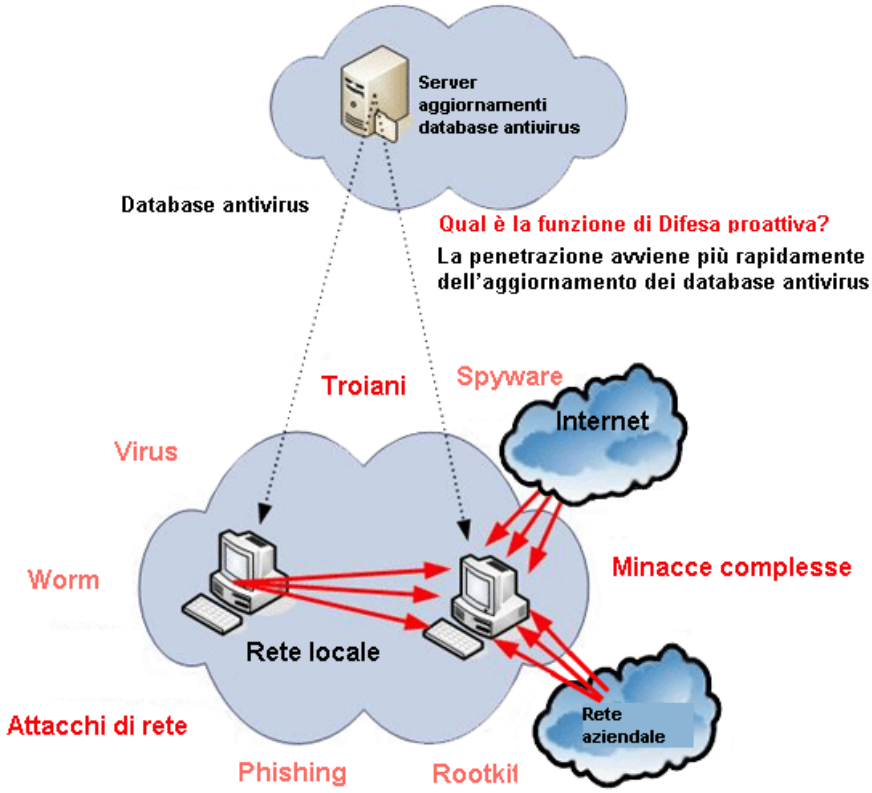
La necessità di un componente come Difesa proattiva si è fatta più pressante man mano che i programmi nocivi hanno iniziato a diffondersi più rapidamente degli aggiornamenti antivirus necessari per neutralizzarli. La tecnica di reazione sulla quale si basano le difese antivirus tradizionali richiede che almeno un computer sia infettato dalla nuova minaccia e comporta il tempo necessario per analizzare il codice nocivo, aggiungerlo al database dell'applicazione e aggiornare il database dei computer degli utenti. A quel punto è possibile che la nuova minaccia abbia già provocato danni notevoli.

Le tecnologie preventive fornite da Difesa proattiva di Kaspersky Internet Security sono in grado di evitare perdite di tempo e neutralizzare le nuove minacce prima che possano danneggiare il computer. Come è possibile? Contrariamente alle tecnologie di reazione che analizzano i codici usando un database dell'applicazione, le tecnologie preventive riconoscono una nuova minaccia nel computer in base alle sequenze di azioni eseguite da una determinata applicazione o processo. L'installazione del programma include una serie di criteri in grado di identificare il livello di pericolosità delle attività di un programma piuttosto che un altro. Se l'analisi dell'attività mostra che le azioni di un certo programma sono sospette Kaspersky Internet Security eseguirà l'azione assegnata dalla regola per quello specifico tipo di attività.

Il set totale delle azioni del programma determina la pericolosità dell'attività. Ad esempio quando l'azione rileva che un programma copia se stesso sulle risorse di rete, nella cartella di avvio o nel registro di sistema e poi invia copie di se stesso è molto probabile che questo programma sia un worm. Comportamenti pericolosi includono anche:

- Modifiche al file system.

- Moduli che vengono incorporati in altri processi.
- Processi di mascheramento nel sistema.
- Modifiche di certe chiavi del registro di sistema di Microsoft Window.



Difesa Proattiva intercetta e blocca tutte le operazioni pericolose usando il set di regole insieme ad un elenco di applicazioni escluse.

In funzione, Difesa proattiva applica una serie di regole incluse nel programma come pure regole create dall'utente durante l'uso del programma. Una *regola* è un insieme di criteri che definiscono un set di comportamenti sospetti e le rispettive reazioni di Kaspersky Internet Security.

Esistono regole individuali per l'attività dell'applicazione e per il monitoraggio delle modifiche al registro di sistema, e i programmi eseguiti sul computer. L'utente può modificare le regole a propria discrezione aggiungendone o

eliminando e modificando quelle esistenti. Le regole possono bloccare azioni o concedere autorizzazioni.

Esaminiamo gli algoritmi di Difesa proattiva:

1. Subito dopo l'avvio del computer, Difesa proattiva analizza i seguenti fattori, usando il set di regole ed esclusioni:

   - *Azioni di ogni applicazione in esecuzione sul computer*. Difesa proattiva registra una cronologia delle azioni eseguite in sequenza e la confronta alle sequenze caratteristiche delle attività pericolose (con il programma è fornito un database dei tipi di attività pericolose che viene aggiornato con i database dell'applicazione).

   - *Integrità dei moduli di programma* dei programmi installati sul computer, che aiuta a impedire la sostituzione dei moduli dell'applicazione a causa dell'incorporazione di codici maligni.

   - *Ogni tentativo di modificare il registro di sistema* eliminando o aggiungendo chiavi del registro di sistema, assegnando strani valori alle chiavi in un formato non ammesso che ne impedisce la visualizzazione o la modifica etc.

2. L'analisi applica le regole di blocco e di consenso di Difesa proattiva.

3. Dopo l'analisi sono disponibili le seguenti possibili azioni:

   - Se l'attività soddisfa le condizioni delle regole di consenso della Difesa proattiva e non incontra alcuna regola di blocco, non viene bloccata.

   - Se l'attività viene gestita come pericolosa sulla base dei criteri pertinenti, il passo successivo dell'applicazione dipenderà dalle istruzioni specificate nella regola: generalmente, l'attività viene bloccata. Sul video viene visualizzato un messaggio che specifica l'applicazione, il tipo di attività svolta dalla stessa e una cronologia delle azioni eseguite. L'utente deve accettare la decisione, bloccare o consentire questa attività. Può inoltre creare una regola per tale attività e annullare le azioni eseguite nel sistema.

     Se l'utente non intraprende alcuna azione quando compare la notifica di Difesa Proattiva, dopo un certo tempo il programma applicherà l'azione predefinita consigliata per quella minaccia. L'azione consigliata può variare a seconda dei tipi di minaccia.

Le categorie di impostazioni (vedi Figura 35) per il componente Difesa Proattiva sono le seguenti:

- *Se l'attività dell'applicazione è monitorata sul computer*

Questa modalità di Difesa proattiva è abilitata spuntando **Abilita Analisi Attività Applicazione**. Per impostazione predefinita, l'analizzatore è abilitato, garantendo un attento monitoraggio delle azioni di qualsiasi programma eseguito sull'host. È possibile configurare l'ordine con cui le applicazioni vengono elaborate per quella attività. Inoltre è possibile creare esclusioni di Difesa proattiva che escludono dal monitoraggio l'attività delle applicazioni selezionate.

- *Se controllo integrità dell'applicazione è abilitato*

Questa funzione tiene sotto controllo l'integrità dei moduli delle applicazioni installate sul computer e viene abilitata selezionando la casella **Abilita Controllo integrità applicazione**. L'integrità viene verificata monitorando il checksum dei moduli dell'applicazione e dell'applicazione stessa. Puoi creare regole (vedi Sezione 10.2 pag. 140) per il monitoraggio dell'integrità dei moduli da qualsiasi applicazione. A tal fine, aggiungere quell'applicazione all'elenco delle applicazioni che devono essere monitorate.

Figura 35. Impostazioni di Difesa proattiva

Questo componente di Difesa Proattiva non è disponibile per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64.

- *Se le modifiche al registro di sistema vengono monitorate*

Per impostazione predefinita, l'opzione **Abilita Controllo del registro** è selezionata, consentendo a Kaspersky Internet Security di

analizzare approfonditamente qualsiasi tentativo di modificare le chiavi di registro del sistema di Microsoft Windows.

L'utente può creare regole proprie (vedi 10.3.2 pag. 147) per monitorare il registro, in base alla chiave di registro.

È possibile inoltre configurare esclusioni (vedi 6.9.1 pag. 83) per i moduli di Difesa proattiva e creare un elenco delle applicazioni attendibili (vedi 6.9.2 a pag. 88).

La seguente sezione prende in esame questi aspetti in maggior dettaglio.

10.1. Regole di monitoraggio della attività

Notare che la configurazione di controllo dell'applicazione per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64 è differente dal processo di configurazione per altri sistemi operativi. Informazioni riguardo la configurazione del controllo dell'attività per questi sistemi operativi è fornita alla fine della sezione.

Kaspersky Internet Security monitora tutte le applicazioni presenti sul computer. L'applicazione incorpora un set di descrizioni degli eventi che possono essere riconosciuti come pericolosi. Per ciascuno di questi eventi è stata creata una regola di monitoraggio. Se l'attività di una certa applicazione viene classificata come evento pericoloso, Difesa Proattiva aderirà strettamente alla regola prevista per quell'evento.

Per monitorare l'attività delle applicazioni, spuntare la casella **Abilita Analisi attività applicazione**.

Osserviamo alcuni tipi di eventi che si verificano nel sistema, e che l'applicazione riconosce come sospetti:

- *Comportamento pericoloso*. Kaspersky Internet Security analizza l'attività delle applicazioni installate sul computer, e rileva le azioni pericolose o sospette da parte dei programmi in base all'elenco di regole creato da Kaspersky Lab. Tali azioni includono, per esempio, l'installazione mascherata di un programma, o i programmi che si copiano da soli.

- *Avvio del browser Internet con parametri*. Analizzando questo tipo di attività, si possono riconoscere i tentativi di aprire un browser con impostazioni. Questa attività è tipica dell'apertura di un browser web da parte di un'applicazione con certe impostazioni del prompt di comando:

ad esempio quando si clicca su un link ad alcuni URL in un messaggio di posta pubblicitario.

- *Intrusione nel processo (invasori).* Consiste nell'aggiungere un codice eseguibile o un flusso supplementare al processo di un determinato programma. Questa attività è tipica dei Trojan.
- *Rilevamento rootkit*. I rootkit sono un insieme di programmi utilizzati per nascondere i programmi nocivi ed i loro processi nel sistema. Kaspersky Internet Security analizza il sistema operativo alla ricerca di processi nascosti.
- *Hook della finestra*. È un'attività utilizzata nei tentativi di lettura di password ed altre informazioni riservate visualizzate nelle finestre di dialogo del sistema operativo. Kaspersky Internet Security identifica tali attività, in caso di tentativi di intercettazione dei dati trasferiti dal sistema operativo alla finestra di dialogo.
- *Valori sospetti nel registro*. Il registro di sistema è un database che memorizza le impostazioni di sistema e dell'utente per controllare il funzionamento di Microsoft Windows, come anche qualsiasi utility stabilita sul computer. I programmi nocivi, cercando di nascondere la loro presenza nel sistema, copiano valori errati nelle chiavi di registro. Kaspersky Internet Security analizza le voci del registro di sistema alla ricerca di valori sospetti.
- *Attività di sistema sospetta*. Il programma analizza le azioni eseguite dal sistema operativo di Microsoft Windows e rileva le attività sospette. Un esempio di attività sospetta potrebbe essere una violazione dell'integrità che modifica uno o più moduli nell'applicazione monitorata rispetto alla sua ultima esecuzione.
- *Rilevamento Keylogger*. È un'attività utilizzata dai programmi nocivi per tentare di leggere password ed altre informazioni riservate digitate per mezzo della tastiera.

L'elenco delle attività pericolose viene aggiornato automaticamente durante l'aggiornamento di Kaspersky Internet Security, ma non può essere modificato dall'utente. È possibile:

- Disabilitare il monitoraggio di una o più attività deselezionando la casella a fianco del nome dell'attività desiderata.
- Modificare la regola utilizzata da Difesa proattiva quando intercetta un'attività pericolosa.
- Creare un elenco di esclusioni (vedi 6.9 a pag. 82) includendovi le applicazioni che non si considerano pericolose.

Configurazione del monitoraggio delle attività,

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Difesa Proattiva** sotto **Protezione**.
2. Cliccare sul pulsante **Impostazioni** nella sezione **Analisi attività applicazione** (vedi Figura 35).

I tipi di attività monitorati da Difesa proattiva sono elencati nella finestra **Analisi attività applicazione: Impostazioni** (vedi Figura 36).

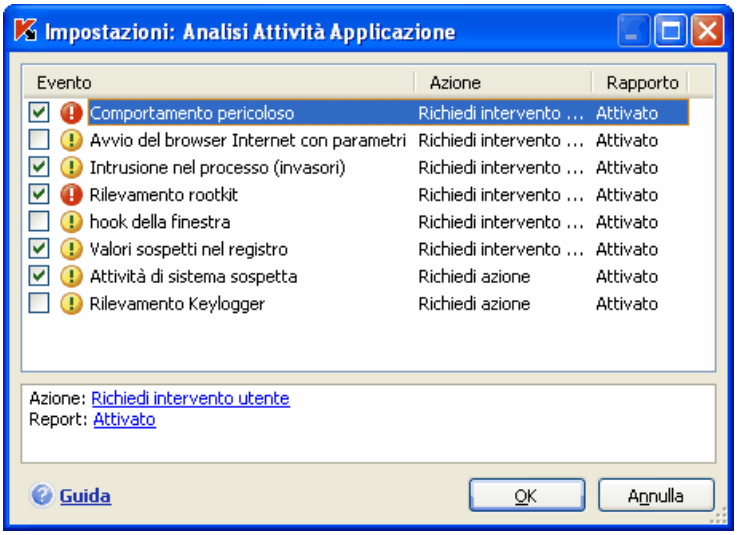


Figura 36. Configurazione dell'analisi dell'attività delle applicazioni

Per modificare un'attività pericolosa, selezionarla dall'elenco e assegnare le impostazioni della regola nella parte inferiore della scheda:

- Assegnare la reazione di Difesa proattiva all'attività pericolosa.

  Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: Permetti, Richiedi intervento utente e Termina. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata. Oltre a terminare il processo è possibile mettere in Quarantena l'applicazione che avvia l'attività pericolosa. Per fare questo usa i link Attivato / Disattivato nelle appropriate impostazioni. È possibile assegnare un valore per determinare la frequenza con cui avverrà la scansione per il rilevamento di processi nascosti nel sistema.

- Stabilire se si desidera generare un report sull'operazione eseguita, cliccando sul link **Report** fino a quando mostra Attivato o Disattivato come richiesto.

Per disabilitare il monitoraggio di un'attività pericolosa, deselezionare la casella accanto al nome dell'attività in questione nell'elenco. Difesa proattiva non analizzerà più il tipo di attività deselezionato.

Specifiche di configurazione dell'analisi attività applicazione in Kaspersky Internet Security per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista o Microsoft Windows Vista x64:

Per i sistemi operativi sopra elencati viene controllato un solo tipo di evento di sistema, *comportamento pericoloso*. Kaspersky Internet Security analizza l'attività delle applicazioni installate sul computer e rileva le attività pericolose o sospette basandosi sull'elenco delle regole creato dagli specialisti di Kaspersky Lab.

Affinché Kaspersky Internet Security monitorizzi l'attività dei processi di sistema oltre ai processi dell'utente, selezionare la casella **Controllo account utente** (vedi Figura 37). Questa opzione è disabilitata per default.

Il controllo degli account dell'utente accede al sistema ed identifica l'utente ed il suo ambiente operativo impedendo ad altri utenti di danneggiare il sistema operativo o i dati. I processi di sistema sono i processi lanciati dall'account dell'utente di sistema.

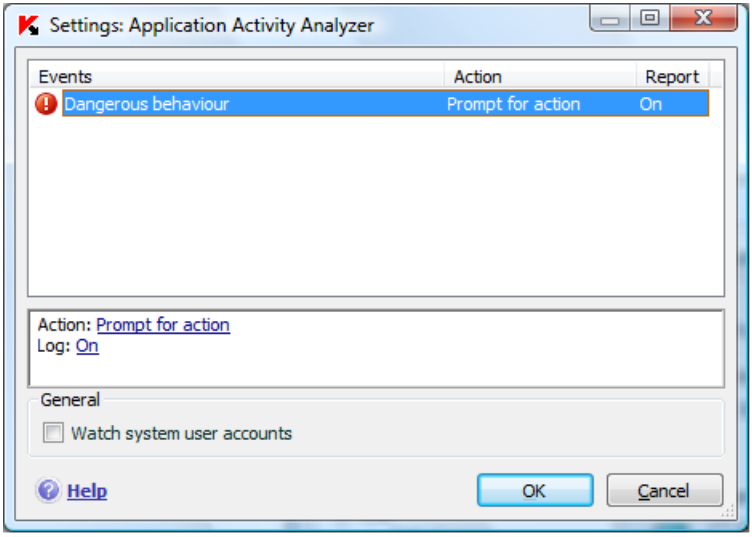


Figura 37. Configurazione dell'analisi attività applicazione per Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64

10.2. Controllo integrità applicazione

Questo componente di Difesa Proattiva non opera su Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista e Microsoft Windows Vista x64.

Esistono diversi programmi fondamentali per il sistema, che potrebbero essere i programmi nocivi potrebbero usare per diffondersi, come browser, client di posta, ecc.. Di norma si tratta di applicazioni e processi di sistema utilizzati per accedere a Internet e per lavorare con la posta elettronica e con altri documenti. È per questo motivo che tali applicazioni sono considerate *critiche* ai fini del controllo delle attività.

Difesa proattiva monitorizza scrupolosamente tali applicazioni ed analizza le loro attività, l'integrità dei moduli di queste applicazioni e osserva gli altri processi avviati dalle stesse applicazioni critiche. Kaspersky Internet Security propone un elenco di applicazioni critiche e per ciascuna di esse una regola di monitoraggio per controllare l'attività dell'applicazione. È possibile aggiungere all'elenco altre applicazioni che l'utente considera critiche, e modificare le regole relative alle applicazioni presenti nell'elenco.

Esiste inoltre un elenco di moduli attendibili che possono venir aperti da tutte le applicazioni controllate. Per esempio i moduli contrassegnati dalla firma digitale di Microsoft Corporation. È altamente improbabile che le attività di applicazioni che includono tali moduli possano essere nocive, pertanto non è necessario monitorarle approfonditamente. Kaspersky Lab ha creato un elenco di questi moduli per alleggerire il carico sul computer durante l'uso di Difesa proattiva.

I componenti contrassegnati dalla firma Microsoft sono aggiunti automaticamente all'elenco delle applicazioni attendibili. Se necessario, è possibile aggiungere o eliminare componenti dall'elenco.

Il monitoraggio dei processi e della loro integrità nel sistema è abilitato spuntando la casella **Abilita Controllo integrità applicazione** nella finestra delle impostazioni di **Difesa Proattiva:** essa è deselezionata per impostazione predefinita. Se si abilita questa funzione, ogni applicazione o modulo di applicazione aperto viene confrontato all'elenco delle applicazioni critiche e attendibili. Se l'applicazione è presente nell'elenco delle applicazioni critiche, la sua attività sarà sottoposta a monitoraggio da parte di Difesa proattiva in accordo con la regola creata per essa.

Per configurare Controllo integrità applicazione:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Difesa Proattiva** sotto **Protezione**.

2. Cliccare sul pulsante **Impostazioni** nella sezione **Controllo integrità applicazione** (vedi Figura 35).

Esaminiamo il lavoro con i processi critici e attendibili.

10.2.1. Configurazione delle regole di Controllo integrità applicazione

Le *applicazioni critiche* sono file eseguibili di programmi il cui monitoraggio è estremamente importante poiché file maligni usano questi programmi per replicarsi.

La scheda **Applicazioni controllate** (vedi Figura 38) contiene un elenco di applicazioni critiche creato al momento dell'installazione del programma. Per ciascuna di tali applicazioni viene creata una regola di monitoraggio. Tali regole possono essere modificate oppure è possibile crearne di nuove.

Difesa proattiva analizza le seguenti operazioni che coinvolgono applicazioni critiche: esecuzione, modifica dei contenuti dei moduli dell'applicazione e avvio di un'applicazione come processo figlio. È possibile selezionare la reazione di Difesa proattiva a ciascuna delle operazioni elencate (Permetti o Blocca) e specificare inoltre se registrare l'attività nel report delle operazioni del componente. Le impostazioni predefinite consentono l'avvio, la modifica o l'avvio come processo figlio della maggior parte delle operazioni critiche.

Per aggiungere un'applicazione critica all'elenco e creare una regola di monitoraggio apposita:

1. Fare clic su **Aggiungi** nella scheda **Applicazioni controllate**. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possibile aprire la finestra di selezione dei file. In alternativa, facendo clic su **Applicazioni** è possibile aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate. L'applicazione viene aggiunta in cima all'elenco. Per impostazione predefinita viene creata per tale applicazione una regola di autorizzazione. La prima volta che questa applicazione viene avviata, viene creato un elenco dei moduli utilizzati all'avvio del programma, ai quali è altrettanto garantita l'autorizzazione mediante la regola **Permetti**.

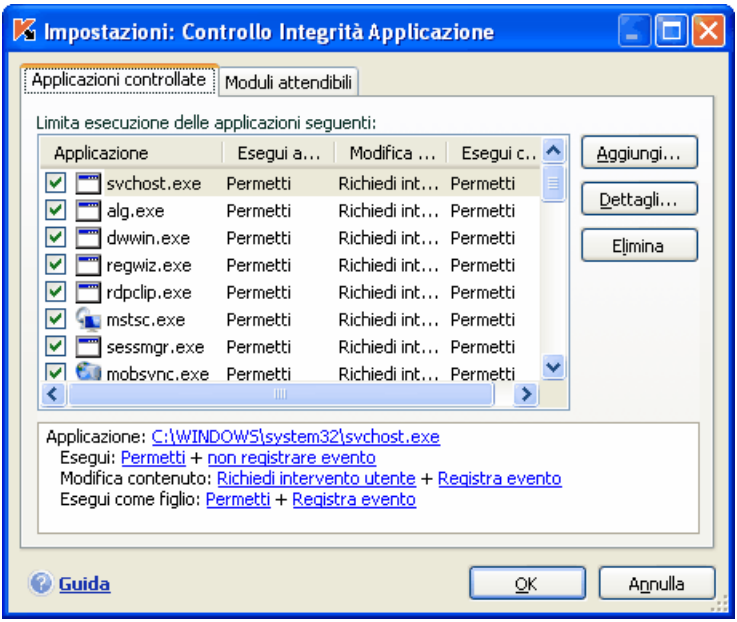


Figura 38. Controllo integrità applicazione

2. Selezionare una regola dall'elenco e assegnare le impostazioni necessarie nella parte inferiore della scheda:

   - Definire la reazione di Difesa proattiva ai tentativi di eseguire una applicazione critica, cambiarne la composizione o avviarsi come processo figlio.

     Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: Permetti, Richiedi intervento utente e Blocca. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata.

   - Stabilire se si desidera generare un report dell'attività, facendo clic su Registra evento / Non registrare evento.

Per disabilitare il monitoraggio dell'attività di un'applicazione, deselezionare la casella ☑ accanto al nome.

Usare il pulsante **Dettagli** per vedere un elenco dettagliato dei moduli per l'applicazione selezionata. La finestra **impostazioni: Moduli applicazione** contiene un elenco dei moduli che vengono usati quando una applicazione monitorata è avviata e compone l'applicazione stessa. Per modificare l'elenco, usare i pulsanti **Aggiungi** ed **Elimina** nella parte destra della finestra.

È inoltre possibile di caricare o bloccare ogni modulo dell'applicazione controllata. Per impostazione viene creata una regola di permesso per ciascun modulo. Per modificare l'azione selezionare il modulo dall'elenco e cliccare sul pulsante **Modifica**. Selezionare l'azione desiderata nella finestra che appare.

Notare che Kaspersky Internet Security esegue l'apprendimento la prima volta che si esegue l'applicazione controllata dopo la sua installazione e fino alla sua chiusura. Il processo di apprendimento produce un elenco dei moduli utilizzati dall'applicazione. Le regole di Controllo Integrità verrà applicate al successivo avvio dell'applicazione.

10.2.2. Creazione di un elenco di componenti comuni

Kaspersky Internet Security include un elenco di componenti comuni che possono essere incorporati in tutte le applicazioni controllate. Questo elenco è consultabile nella scheda **Moduli attendibili** (vedi Figura 39). L'elenco contiene i moduli utilizzati da Kaspersky Internet Security, i componenti con firma di Microsoft : componenti che possono essere aggiunti o rimossi dall'utente.

Se si installano dei programmi sul computer, è possibile garantire che quelli contenenti moduli firmati da Microsoft siano automaticamente aggiunti all'elenco dei moduli attendibili. A tal fine, selezionare la casella  **Aggiungi automaticamente componenti firmati da Microsoft Corporation a questo elenco**. Poi, se un'applicazione controllata tenta di caricare un modulo firmato da Microsoft, il programma ne consente automaticamente il caricamento e il modulo viene inserito nell'elenco di componenti condivisi.

Per aggiungere un modulo all'elenco dei moduli attendibili, fare clic su **Aggiungi** e selezionare il modulo nella finestra standard di selezione file.

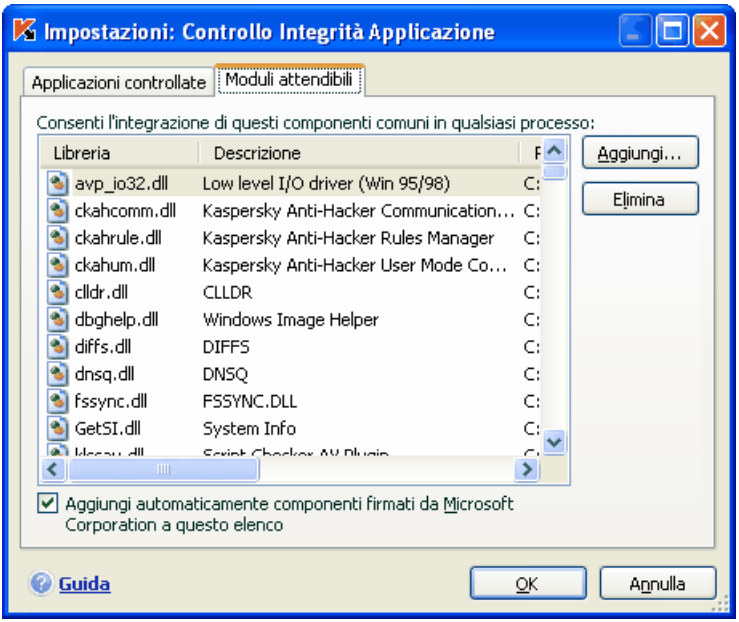


Figura 39. Configurazione dell'elenco dei moduli attendibili

10.3. Controllo del registro

Uno degli obiettivi di molti programmi nocivi è quello di modificare i registri di sistema di Microsoft Windows sul computer. Può trattarsi di innocui programmi-scherzo, così come di programmi realmente nocivi che rappresentano un'autentica minaccia per il computer.

Per esempio, programmi maligni possono copiare le proprie informazioni sulle chiavi di registro che determinano l'apertura automatica delle applicazioni all'avvio. Così facendo, i programmi maligni partiranno automaticamente all'avvio del sistema operativo.

Lo speciale modulo di Difesa proattiva tiene traccia delle modifiche degli oggetti del registro di sistema. Questo modulo può essere abilitato o disabilitato spuntando la casella ☑ **Abilita Controllo del registro**.

Per configurare il monitoraggio dei registri di sistema:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Difesa Proattiva** sotto **Protezione**.

2. Cliccare sul pulsante **Impostazioni** nella sezione **Controllo del registro** (vedi Figura 35).

Kaspersky Lab ha già creato un elenco di regole per controllare le operazioni del file di registro e lo ha incluso nel programma. Le operazioni relative alle chiavi di registro sono catalogate in gruppi logici come *System Security*, *Internet Security*, ecc. Ognuno di questi gruppi elenca i file del registro del sistema e regole per lavorare con essi. Ogni volta che il programma viene aggiornato, si aggiorna anche questo elenco.

La finestra delle impostazioni del **Controllo del registro** (vedi Figura 40) fornisce un elenco completo di regole.

Ad ogni gruppo di regole è assegnata una priorità di esecuzione che è possibile modificare per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Più alto il gruppo è nell'elenco più alta è la priorità assegnata ad esso. Se il medesimo file di registro appartiene a gruppi diversi la prima regola applicata a quel file sarà quella del gruppo a più elevata priorità.

Per arrestare l'uso di qualsiasi gruppo di regole, procedere come segue:

- Deselezionare la casella ☑ accanto al nome del gruppo. Il gruppo di regole rimane presente nell'elenco ma non utilizzato.
- Eliminare il gruppo di regole dall'elenco. Si sconsiglia di eliminare i gruppi creati da Kaspersky Lab poiché contengono gli elenchi dei file del registro di sistema più spesso usati dai programmi maligni.

Figura 40. Gruppi chiavi di registro controllati

L'utente può creare gruppi di file di registro monitorati personalizzati. A tal fine, cliccare su **Aggiungi** nella finestra dei gruppi di file.

Nella finestra che si apre eseguire questi passaggi:

1. Digitare il nome del nuovo gruppo di file per il monitoraggio delle chiavi di registro del sistema nel campo **Nome del gruppo**.
2. Selezionare la scheda **Chiavi** e creare un elenco di file di registro che apparterranno al gruppo da monitorare (vedi 10.3.1 pag. 146) per il quale si desidera creare la regola. Può trattarsi di una o più chiavi.
3. Selezionare il tasto **Regole** e creare una regola (vedi 10.3.2 pag. 147.) per i file che verranno applicati alla chiave selezionata. È possibile creare più regole e impostarne l'ordine di applicazione.

10.3.1. Selezione delle chiavi di registro per creare una regola

Il gruppo di file creato deve contenere almeno un file di registro di sistema. La scheda **Chiavi** contiene un elenco di file per la regola.

Per aggiungere una chiave di registro del sistema:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Modifica** (vedi Figura 41).
2. Nella finestra che si apre selezionare il file di registro o la cartella o i file per cui si desidera creare la regola di monitoraggio.
3. Specificare il valore dell'oggetto o maschera per il gruppo di oggetti a cui si desidera applicare la regola nel campo **Valore**.
4. Selezionare la casella **Includi sottochiavi** per applicare la regola a tutti i file allegati al file di registro elencato.

È necessario utilizzare maschere con un asterisco e un punto interrogativo contemporaneamente all'opzione **Includi sottochiavi** solo quando i caratteri jolly sono utilizzati nel nome della chiave.

Se si seleziona una cartella di file di registro che utilizzano una maschera e ne specificano un valore, la regola sarà applicata a quel valore per tutte le chiavi del gruppo selezionato.

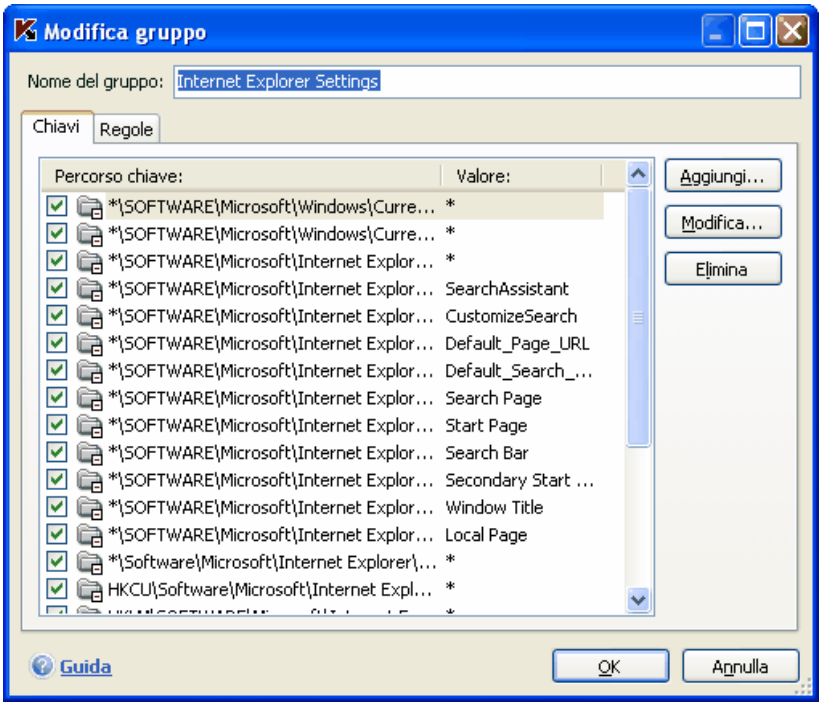


Figura 41. Aggiunta di chiavi di registro controllate

10.3.2. Creazione di una regola per Controllo del registro

Una regola di Controllo del registro specifica:

- Il programma il cui accesso al registro di sistema viene monitorato.
- La reazione di Difesa Proattiva quando un programma tenta di eseguire un'operazione con un file di registro di sistema.

Per creare una regola per i file di registro del sistema selezionati:

1. Fare clic su **Nuovo** nella scheda **Regole**. La regola generale sarà aggiunta in cima all'elenco delle regole (vedi Figura 42).
2. Selezionare una regola dall'elenco e assegnare le impostazioni necessarie nella parte inferiore della scheda:
    - Specificare l'applicazione.

La regola viene creata per qualsiasi applicazione per impostazione predefinita. Se si desidera applicare la regola a un'applicazione specifica, fare clic con il pulsante sinistro del mouse su any che diventa selezionata. Quindi cliccare sul link specificare nome applicazione. Si apre un menu contestuale. Cliccare su **Sfoglia** per aprire la finestra standard di selezione dei file oppure cliccare su **Applicazioni** per vedere un elenco di applicazioni aperte e selezionare una di esse come desiderato.

- Definire la reazione di Difesa proattiva per l'applicazione selezionata che cerca di leggere, modificare o eliminare i file del registro di sistema.

  Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: Permetti, Richiedi intervento utente e Blocca. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata.

- Stabilire se si desidera generare un report dell'operazione eseguita, facendo clic su registra evento / non registrare evento.

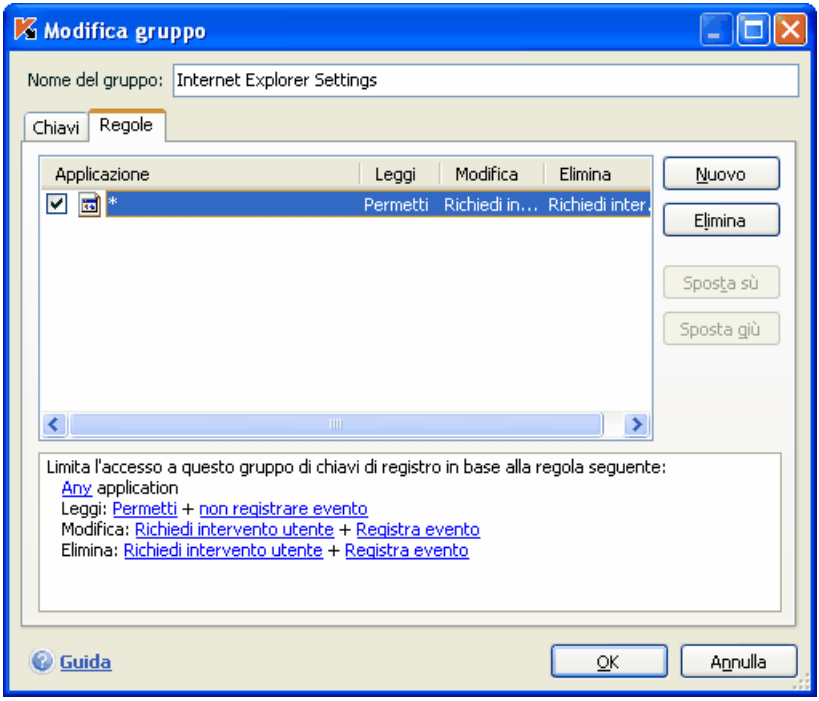


Figura 42. Creazione di una regola di monitoraggio delle chiavi di registro

È possibile creare diverse regole e modificarne la priorità per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Più alta è la regola nell'elenco, maggiore sarà la priorità assegnata ad essa.

È possibile inoltre creare una regola di autorizzazione (ad esempio tutte le azioni sono permesse) per un oggetto del registro di sistema da una notifica che comunica che un programma sta tentando di eseguire unìoperazione con un oggetto. A tal fine, fare clic nella finestra che si apre su Crea regola di autorizzazione nell'avviso e specificare l'oggetto del registro di sistema al quale la regola verrà applicata.

CAPITOLO 11. PROTEZIONE CONTRO LE FRODI INTERNET

Il componente di Kaspersky Internet Security che protegge da tutti i tipi di malware è chiamato Controllo Privacy. Recentemente i malware includono sempre di più programmi il cui scopo è:

- Sottrarre informazioni riservate, comprese password, numeri di carta di credito, documenti importanti etc.
- Tenere traccia delle azioni dell'utente sul computer ed analizzare il software installato.
- Ottenere accessi non autorizzati in Internet dal computer dell'utente a diversi siti web.

Phishing e keylogger si focalizzano sul sottrarre informazioni riservate; mentre autodialer, programmi joke e adware sono volti a sottrarre all'utente tempo e denaro. Controllo Privacy è progettato per difendersi da questi programmi.

Controllo Privacy comprende i seguenti moduli:

- Il componente *Anti-Phishing,* che protegge dal phishing.

  Il phishing generalmente consiste in e-mail inviate da ipotetici istituti finanziari che contengono collegamenti ai loro siti web. Il messaggio convince il lettore ad aprire un collegamento ed inserire informazioni riservate nella pagina web, per esempio, il numero di una carta di credito oppure i dati di connessione al sito di una vera banca.

  Un comune esempio di phishing è una e-mail che sembra essere stata inviata dalla banca dell'utente, con un collegamento al sito ufficiale. Cliccando sul link ci si ritrova su una copia esatta del sito della banca e si riconosce addirittura l'indirizzo nella barra degli indirizzi del browser ma, in realtà, si tratta di un sito contraffatto. Da questo momento tutte le azioni compiute sul sito sono tracciate e possono essere usate per sottrarre denaro all'utente.

  Il collegamento ad un sito di phishing può pervenire via e-mail oppure attraverso un programma di instant messaging. Anti-Phising controlla i tentativi di aprire i siti di phishing e li blocca.

  I database di Kaspersky Internet Security comprendono gli indirizzi di tutti i siti di phishing correntemente noti. Gli specialisti di Kaspersky Lab

alimentano l'elenco con gli indirizzi messi a disposizione da Anti-Phishing Working Group, una organizzazione internazionale. I siti vengono aggiunti all'elenco aggiornando i database dell'applicazione.

- *Anti-Dialer* protegge il computer contro i tentativi di eseguire connessioni modem non autorizzate.

  I dialer generalmente stabiliscono delle connessioni con specifici siti, come siti a contenuto pornografico. L'utente è così obbligato a pagare per un costoso traffico che non ha mai avuto intenzione di usare. Per escludere un numero dall'elenco delle connessioni bloccate, occorre inserirlo nell'elenco dei numeri consentiti (vedi 11.1 pag. 152).

- Il modulo Controllo Privacy intercetta i tentativi di trasmissione non autorizzata di informazioni riservate dal computer dell'utente (vedi Sezione 11.2 pag. 153).

  Informazioni riservate comprendono, soprattutto, dati memorizzati nella Windows Protected Storage (password locali, password della posta, informazioni a completamento automatico, ecc.).

  Inoltre il modulo Controllo Privacy analizza ogni tentativo di trasmettere informazioni dal computer dell'utente usando un processo nascosto come un web browser.

Figura 43. Impostazioni Controllo Privacy

11.1. Creazione di un elenco di numeri attendibili per Anti-Dialer

Il componente *Anti-Dialer* monitora i numeri di telefono utilizzati per collegarsi a Internet all'insaputa dell'utente. Una connessione è considerata "segreta" se è configurata in modo tale da non informare l'utente della connessione o se si tratta di una connessione non lanciata dall'utente.

Ad ogni tentativo di connessione segreta, il programma ne informa l'utente emettendo uno speciale messaggio sul video in cui chiede se bloccare o permettere la chiamata. Se non è stato l'utente stesso a lanciare la connessione, è molto probabile che sia stata configurata da un programma maligno.

Per permettere la connessione a determinati numeri senza che sia richiesta ogni volta la conferma, l'utente deve aggiungere tali numeri all'elenco dei numeri attendibili. A tal fine:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Controllo Privacy** sotto **Protezione**.
2. Spuntare **Abilita Anti-Dialer** e cliccare sul pulsante **Numeri attendibili** sotto **Anti-Dialer** (vedi Figura 43).
3. Cliccare su **Aggiungi** nella corrispondente finestra di dialogo (vedi Figura 44). Specificare il numero oppure la maschera del numero che deve essere consentito nella finestra **Nuovo numero di telefono**.

Figura 44. Creazione di un elenco di indirizzi attendibili

Suggerimento:

Quando si immette una maschera per un numero attendibile, è possibile utilizzare i caratteri * o ?.

Ad esempio +???? 79787* coprirà tutti i numeri che iniziano per 79787 ed i cui prefissi di zona sono composti da quattro cifre.

Il nuovo numero telefonico sarà aggiunto in testa all'elenco dei numeri attendibili. Per interrompere l'esclusione del numero aggiunto, è sufficiente deselezionare la casella ☑ corrispondente nell'elenco. Per eliminare completamente una esclusione. selezionarla nell'elenco e cliccare su **Elimina**.

11.2. Tutela dei dati riservati

Il modulo Controllo Privacy comprende un modulo di *Tutela dei dati riservati* che protegge le informazioni confidenziali dell'utente da accessi o trasmissioni non autorizzati.

Per abilitare i moduli selezionare ☑ **Abilita Tutela Dati Riservati** nella finestra delle impostazioni di **Controllo Privacy** (vedi Figura 43).

Il modulo controlla i seguenti metodi di accesso ai dati riservati:

- *Tentativo di inviare dati personali*.

  Per inviare dati con questo metodo i codici maligni avviano un processo nascosto sul computer dell'utente, generalmente un browser web, come *iexplorer.exe*. Poiché il Firewall permette sempre l'attività di questi programmi, in apparenza questi processi non sono indicativi di eventuali minacce. Questo processo serve per trasmettere i dati dal computer attraverso il protocollo http. I dati vengono estratti dal file corrispondente e criptati per la trasmissione.

- *Tentativo di accedere a dati personali o password contenute in Protected Storage.*

  Questo strumento di Microsoft Windows archivia i dati segreti, come password locali, password POP ed SMTP della posta, password di accesso ad Internet, password per collegamenti ad aree protette o siti web, password di auto-completamento etc.

  Queste informazioni sono inserite nei corrispondenti file della posta e del browser. Di solito l'utente può salvare salvare le informazioni in questi campi di immissione, spuntando una casella di selezione. In questo caso Microsoft Windows salva i dati introdotti nel Protected Storage.

  Vale la pena di notare che anche gli utenti che temono la perdita di dati dal Protected Storage e per questa ragione non salvano password e dati nel browser. normalmente salvano le password e-mail poichè il doverle digitare ogni volta che spediscono o ricevono una e-mail richiederebbe molto più tempo. Considerando che gli ISP spesso hanno accessi protetti ad Internet ed alle password e-mail, il ritrovarle potrebbe permettere l'accesso sia alle caselle di posta che alla connessione Internet dell'utente.

  Le informazioni contenute in Protected Storage possono essere estratte usando speciali spyware e quindi essere inviate agli hacker. Per impedire ciò il modulo di Tutela dei dati riservati notifica ogni tentativo di leggere dati di Protected Storage da parte di una applicazione che non dispone della firma digitale di Microsoft Corporation. In funzione del livello di attendibilità attribuito all'applicazione che sta tentando di accedere alle informazioni contenute in quell'area di memoria, l'utente può permettere o bloccare l'esecuzione dell'operazione.

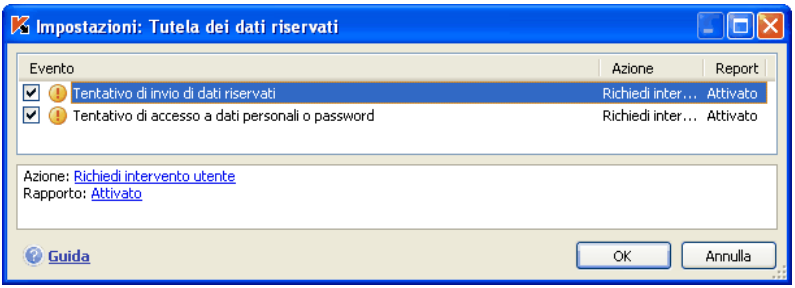


Figura 45. Impostazioni: Tutela dei dati riservati

Per configurare le impostazioni di Tutela dei dati riservati, effettuare i passaggi seguenti:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Controllo Privacy** sotto **Protezione**.
2. Spuntare ☑ **Abilita Tutela dei dati riservati** e cliccare su **Impostazioni** sotto **Tutela dei dati riservati** (vedi Figura 45).

Nella finestra **Impostazioni: Tutela dei dati riservati**, selezionare le caselle corrispondenti agli eventi che il modulo dovrebbe monitorare. Per arrestare il monitoraggio di un evento, deselezionare la casella ☑ vicino al suo nome nell'elenco.

Per modificare una regola di monitoraggio dell'accesso ai dati riservati selezionarla dall'elenco ed assegnare le impostazioni per la regola nella parte inferiore della finestra:

- Definizione della reazione del modulo Controllo Privacy a quell'evento.

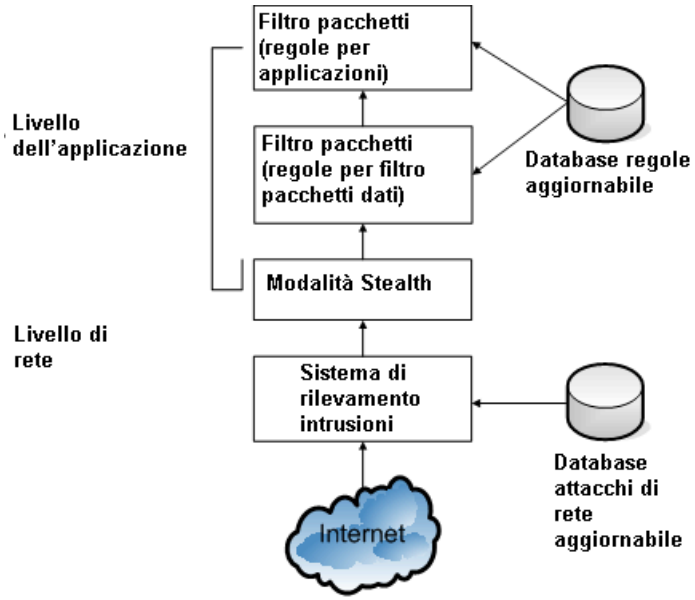
  Come reazione, è possibile assegnare una qualsiasi delle seguenti azioni: nega, permetti, richiedi intervento utente o termina. Cliccare con il tasto sinistro sul collegamento dell'azione fino a raggiungere il valore desiderato. Oltre ad arrestare il processo, è possibile mettere in quarantena l'applicazione che tenta l'accesso ai dati. A tal fine, utilizzare i link Attivato / Disattivato della relativa impostazione.

- Scegliere se generare un report dell'operazione svolta. A tal fine, fare clic su Attivato / Disattivato.

CAPITOLO 12. PROTEZIONE CONTRO GLI ATTACCHI DI RETE

I computer di oggi sono diventati estremamente vulnerabili durante la navigazione in Internet. sono soggetti a infezioni virali e ad altri tipi di attacco che sfruttano le vulnerabilità dei sistemi operativi e del software.

Kaspersky Internet Security contiene uno speciale componente, *il Firewall*, che garantisce la sicurezza sulle reti locali (LAN) e in Internet. Questo componente protegge il computer a livello di rete e di applicazioni, e lo maschera su Internet per evitare gli attacchi. Osserviamo in dettaglio il funzionamento del Firewall.



Il computer è protetto a livello di rete grazie a regole di filtro pacchetti che autorizzano o bloccano l'attività di rete in base all'analisi delle impostazioni quali la direzione di un pacchetto, il protocollo di trasferimento del pacchetto di dati e la porta del pacchetto in uscita. Le regole per i pacchetti di dati stabiliscono l'accesso alla rete indipendentemente dalle applicazioni installate sul computer che fanno uso della rete.

Oltre alle regole di filtro pacchetti, anche Intrusion Detection System (IDS) offre una protezione supplementare a livello di rete. L'obiettivo del sistema è analizzare le connessioni in entrata, rilevare le scansioni delle porte del computer e filtrare i pacchetti di rete volti a sfruttare le vulnerabilità del software. Quando è in esecuzione, Intrusion Detection System blocca tutte le connessioni in entrata provenienti da un determinato computer per un tempo specificato, e l'utente riceve un messaggio che lo informa del tentativo di attacco di rete subito dal computer.

Intrusion Detection System si basa sull'uso di uno speciale database degli attacchi di rete (vedi 12.1.3 a pag. 177) per l'analisi, aggiornato regolarmente dal nostro team. Esso viene aggiornato con i database dell'applicazione.

Il computer è protetto a livello di applicazioni grazie alle regole sull'uso delle risorse di rete per le applicazioni installate sul computer. Come per la sicurezza a livello di rete, la sicurezza a livello di applicazioni si basa sull'analisi dei pacchetti dati dal punto di vista di direzione, protocollo di trasferimento e porte utilizzate. Tuttavia, a livello di applicazioni, vengono prese in considerazione anche le caratteristiche del pacchetto dati e l'applicazione specifica che invia e riceve il pacchetto.

L'uso delle regole delle applicazioni agevola la configurazione di una protezione più specifica quando, per esempio, un determinato tipo di connessione viene precluso ad alcune applicazioni ma non ad altre.

Esistono due tipi di regole per il Firewall, basati sui due livelli di sicurezza di Anti-Hacker:

- *Regole per filtro pacchetti* (vedi 12.1.1.3 pag. 166). Utilizzate per creare restrizioni di carattere generale all'attività di rete, a prescindere dalle applicazioni installate. Esempio: se si crea una regola di filtro pacchetti che blocca le connessioni in entrata sulla porta 21, nessuna delle applicazioni che utilizza quella porta (un server ftp, per esempio) sarà accessibile dall'esterno.
- *Regole per applicazioni* (vedi 12.1.1.2 pag. 161). Utilizzate per creare restrizioni all'attività di rete per applicazioni specifiche. Esempio: se sono attive delle regole di blocco delle connessioni sulla porta 80 per tutte le applicazioni, è possibile creare una regola che consenta le connessioni su tale porta a Firefox (o a un altro browser).

Esistono due tipi di regole per applicazioni e filtro pacchetti: *permetti* e *blocca*. L'installazione del programma include una serie di regole volte a regolare l'attività di rete per la maggior parte delle applicazioni, che utilizza i protocolli e le porte più comuni. Kaspersky Internet Security include inoltre una serie di regole di autorizzazione per applicazioni attendibili la cui attività di rete non dà adito a sospetti.

Kaspersky Internet Security suddivide l'intero spazio di rete in zone, in modo da semplificare le impostazioni e le regole: *Internet* e *zone di sicurezza*, che

corrispondono in gran parte alle sottoreti di cui il computer fa parte. È possibile assegnare uno stato a ogni zona (*Internet, Local Area Network, attendibile*), dal quale dipenderà l'applicazione delle regole e il monitoraggio delle attività di rete nelle singole zone (vedi 12.1.1.5 pag 172).

Una speciale funzione del Firewall, la *modalità Stealth* (modalità invisibile), impedisce il rilevamento del computer dall'esterno, privando così gli hacker da un obiettivo da attaccare. Questa modalità non influisce sulle prestazioni del computer in Internet, a condizione che non sia utilizzato come server, nel qual caso la modalità Stealth è sconsigliata.

In più, è emerso che numerosi programmi sono progettati per trasmettere inopportunamente contenuti pubblicitari nei browser web. Questi programmi non costituiscono una minaccia diretta. Piuttosto, congestionano il traffico con conseguente perdita di tempo e di denaro per l'utente.

Il Firewall comprende due moduli: Anti-Pubblicità (vedi 12.1.3 pag 177) e Anti-Banner (vedi 12.1.4 pag 179) che filtrano il traffico contro la pubblicità insistente. Recentemente sono emersi una moltitudine di programmi che visualizzano varie pubblicità nella finestra del browser, nelle finestre pop-up e nei banner. Questi programmi non costituiscono una minaccia diretta ma incrementano il traffico, causano perdite di tempo agli utenti che ne subiscono dei danni.

12.1. Configurazione del Firewall

Durante la navigazione il computer è protetto dai seguenti moduli del Firewall:

- Sistema di filtro (vedi 12.1.1 pag. 159) che filtra, a livello di rete (pacchetto) e di applicazione (programma), il traffico in entrata ed uscita.

  Il traffico è filtrato sulla base del livello di sicurezza configurato ed un continuo aggiornamento dei database delle regole di permesso o di blocco. Per semplificare la configurazione della regola e dell'applicazione, la globalità della rete è ripartita in aree di sicurezza in funzione del rischio associato.

- Sistema di rilevamento delle intrusioni (vedi 12.1.2 pag. 176) che protegge il computer da tutte le minacce note al momento. Il database delle minacce è continuamente aggiornato dagli specialisti di Kaspersky Lab e gli aggiornamenti vengono scaricati con i database dell'applicazione.

- Modulo Anti-Pubblicità (vedi Sezione 12.1.3 pag. 177) che blocca i pop-up.

- Modulo Anti-Banner (vedi 12.1.4 pag. 179) che blocca i banner.

Tutti i moduli del Firewall sono abilitati per impostazione predefinita. Il Firewall o i suoi singoli moduli possono essere disabilitati e configurati. A tal fine:

aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**. Per attivare il Firewall spuntare **Abilita Firewall.** I singoli moduli possono essere abilitati/disabilitati e impostati con precisione nell'appropriata area della finestra impostazioni (vedi Figura 46).

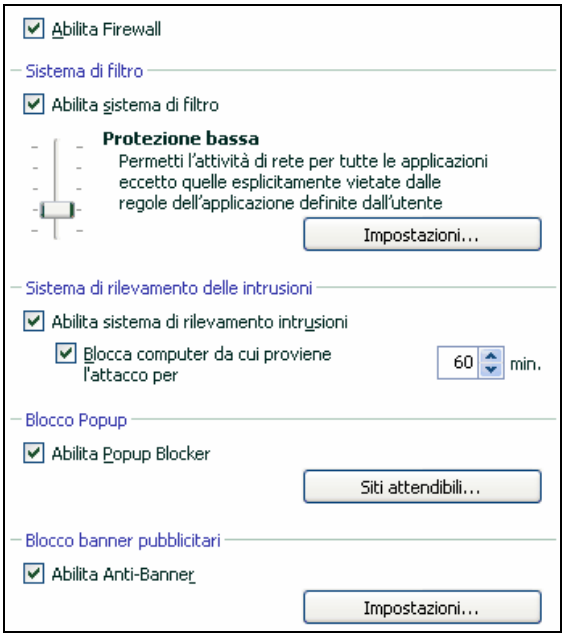


Figura 46 . Configurazione Firewall

12.1.1. Configurazione dei filtri

Il Sistema di filtro è un modulo del Firewall che protegge il computer durante la connessione a Internet. Questo modulo filtra il traffico in entrata ed in uscita a livello di rete/pacchetto e applicazioni. Il traffico viene filtrato usando un database aggiornabile di regole di "permesso" e di "blocco". Per configurare ed applicare facilmente le regole tutto lo spazio della rete è diviso in zone di sicurezza secondo il relativo grado di rischio.

Le seguenti impostazioni possono essere configurate per il sistema di filtro:

- Livello di protezione dagli attacchi di rete (vedi 12.1.1.1 pag. 160).
- Regole per applicazioni (vedi 12.1.1.2 pag. 161).

- Regole per filtri pacchetti (vedi 12.1.1.3 pag. 166).
- Regole per zone di sicurezza (vedi 12.1.1.6 pag. 172).
- Modalità Firewall (vedi Sezione 12.1.1.7 pag. 175).

12.1.1.1. Selezione di un livello di sicurezza

Quando il computer lavora in rete. Kaspersky Internet Security lo protegge ad uno dei seguenti livelli:

Blocca tutto – blocca qualsiasi attività di rete sul computer. Se si è selezionato questo livello di sicurezza, non sarà possibile utilizzare nessuna risorsa di rete o programma che richiedano una connessione in rete. Si raccomanda di selezionare questo livello solo in caso di attacco di rete o durante l'uso di una rete pericolosa su una connessione non protetta.

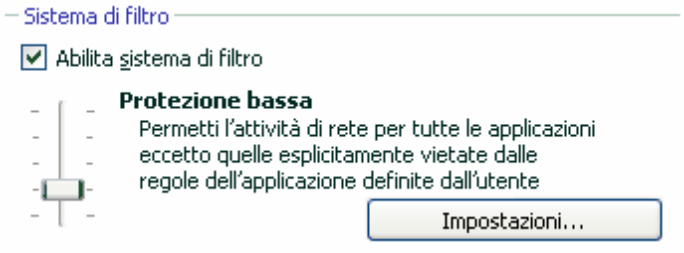


Figura 47. Selezione di un livello di protezione del Firewall

Protezione alta – l'attività di rete è possibile nella misura consentita dalle regole di permesso. Il Firewall utilizza regole preimpostate o personalizzate. La serie di regole predefinite di Kaspersky Internet Security include regole di permesso per applicazioni la cui attività di rete non è sospetta e per pacchetti dati assolutamente sicuri da inviare e da ricevere. Se tuttavia nell'elenco delle regole esiste una regola di blocco per un'applicazione con priorità più elevata rispetto a quella di blocco, il programma blocca ogni attività di rete dell'applicazione.

Attenzione!

Se si seleziona questo livello di sicurezza, tutte le attività di rete non registrate in una regola di permesso di Firewall saranno bloccate. Si raccomanda quindi di utilizzare questo livello solo se si è certi che tutti i programmi di cui si necessita sono autorizzati dalle regole a stabilire connessioni di rete e se non si progetta di installare nuovo software.

Modalità Apprendimento – livello di sicurezza dove vengono create le regole per il Firewall. A questo livello, ogni volta che un programma tenta di utilizzare una risorsa di rete il Firewall controlla se esiste una regola per tale connessione. In presenza di una regola, il Firewall la applica. In assenza di regole, viene visualizzato un messaggio contenente una descrizione della connessione di rete (il programma che l'ha avviata, la porta utilizzata, il protocollo, ecc.). L'utente deve decidere se autorizzare la connessione oppure no. Per mezzo di un apposito pulsante nella finestra del messaggio, è possibile creare una regola per tale connessione in modo che, in futuro, il Firewall applicherà le condizioni della regola senza più avvertire l'utente.

Protezione bassa – blocca solo le attività di rete bandite, in base alle regole di blocco incluse nel programma o create dall'utente. Se tuttavia nell'elenco delle regole esiste una regola di autorizzazione per un'applicazione con priorità più elevata rispetto a quella di blocco, il programma autorizzerà l'attività di rete di quell'applicazione.

Consenti tutto – autorizza qualsiasi attività di rete sul computer. Si raccomanda di limitare l'uso di questo livello a casi estremamente rari in cui non si osservino attacchi attivi di rete e sia quindi possibile ritenere affidabile tutta l'attività di rete.

È possibile aumentare o ridurre il livello di sicurezza della rete selezionando quello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza della rete:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.
2. Regolare il cursore sotto **Abilita Sistema di filtro** nel pannello di destra della finestra (vedi Figura 47).

Per configurare il livello di sicurezza della rete:

1. Selezionare il livello di sicurezza che meglio soddisfa le proprie esigenze.
2. Cliccare sul pulsante **Impostazioni** sotto **Sistema di filtro** e modificane le impostazioni nella finestra di dialogo **Impostazioni**: **Firewall**.

12.1.1.2. Regole delle applicazioni

Kaspersky Internet Security include una serie di regole per le applicazioni DI Microsoft Windows più comuni. È possibile creare più regole di permesso e di blocco per lo stesso programma. Si tratta solitamente di programmi con attività di rete che sono state analizzate in dettaglio dagli esperti Kaspersky Lab e definite come decisamente pericolose o attendibili.

A seconda del livello di sicurezza (vedi 12.1.1.1 pag. 160) selezionato per la Firewall e del tipo di rete (vedi 12.1.1.5 pag 172) di cui fa parte il computer, l'elenco delle regole per i programmi può essere utilizzato in vari modi, per esempio applicando solo regole di autorizzazione con il livello di **Protezione alta**. Tutte le attività di rete delle applicazioni che non corrispondono alle regole vengono bloccate.

Per lavorare con l'elenco delle regole per applicazioni:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione** (vedi Figura 47).
2. Cliccare su **Impostazioni** sotto **Abilita Sistema di filtro**.
3. Selezionare la scheda **Regole per applicazioni** nella finestra di dialogo **Impostazioni: Firewall** (vedi Figura 51).

Tutte le regole di questa scheda possono essere raggruppate in uno dei due seguenti criteri:

- *Regole per applicazioni* – Se l'opzione **Raggruppa regole per applicazione** è selezionata, l'elenco delle regole è visualizzato in base alle applicazioni. La scheda contiene in questo caso un elenco di applicazioni per le quali sono state create delle regole. Per ogni applicazione sono riportate le seguenti informazioni: nome e icona dell'applicazione, prompt di comando, root directory in cui si trova il file eseguibile dell'applicazione e il numero di regole create.

  Per mezzo del pulsante **Modifica**, è possibile aprire l'elenco delle regole per l'applicazione selezionata e modificarlo: aggiungere una nuova regola, modificare le regole esistenti e cambiare le priorità.

  Per mezzo del pulsante **Aggiungi**, è possibile aggiungere una nuova applicazione all'elenco e creare una regola apposita.

  I pulsanti **Esporta** e **Importa** sono progettati per consentire di trasferire le regole create da un computer a un altro e accelerare la configurazione del Firewall.

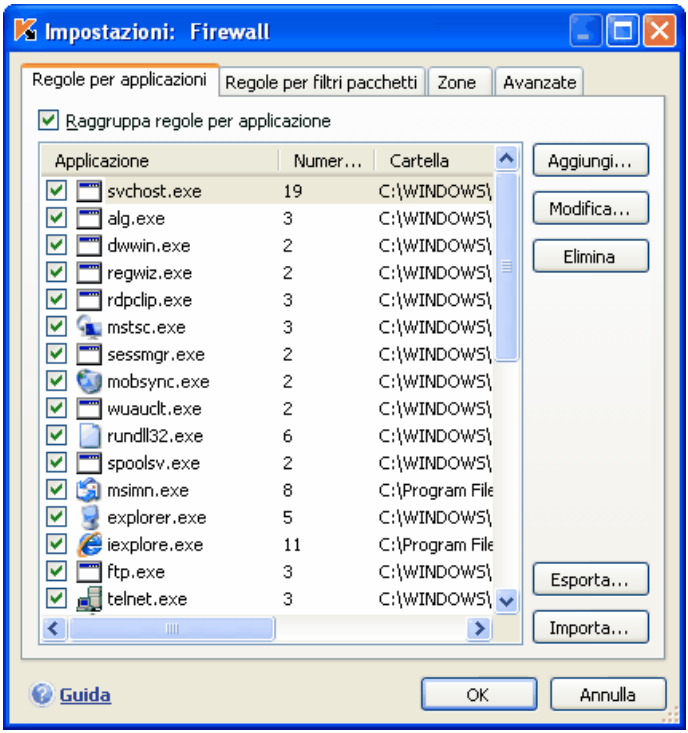


Figura 48. Elenco di regole per le applicazioni installate sul computer

- *Elenco generale* delle regole. Se l'opzione **Raggruppa regole per applicazione** è deselezionato, allora ciascuna riga dell'elenco generale mostra le informazioni per la regola: il nome dell'applicazione e il comando per avviarla, permesso o blocco dell'attività di rete, il protocollo di trasferimento dati, la direzione dei dati (in entrata o in uscita) e altre informazioni.

  Il pulsante **Aggiungi** consente di creare nuove regole, mentre per modificare una regola selezionata dall'elenco è possibile usare il pulsante **Modifica**. È possibile inoltre modificare le impostazioni base nella parte inferiore della scheda.

  Servirsi dei pulsanti **Sposta su** e **Sposta giù** per cambiare la priorità delle regole.

12.1.1.2.1. Creazione manuale delle regole

Per creare manualmente una regola per applicazioni:

1. Selezionare l'applicazione facendo clic sul pulsante **Aggiungi** sulla scheda **Regole per applicazioni**. Apparirà un menu contestuale che porterà ad una finestra di selezione di file standard attraverso la voce **Sfoglia** oppure ad un elenco di applicazioni attive attraverso la voce **Applicazioni** per eseguire la selezione. Si apre un elenco di regole per l'applicazione selezionata. Se esistono già delle regole per l'applicazione, esse sono elencate nella parte superiore della finestra. In assenza di regole, la finestra appare vuota.
2. Fare clic sul pulsante **Aggiungi** nella finestra delle regole per l'applicazione selezionata.

Nella finestra **Nuova regola** che si apre è presente un modulo utilizzabile per mettere a punto con precisione i criteri di una regola (vedi 12.1.1.6 pag. 172).

12.1.1.2.2. Creazione di regole da un modello

Anti-Virus include modelli per regole già pronti che possono essere utilizzati per creare regole personalizzate.

L'intera gamma di applicazioni di rete esistente può essere suddivisa in vari tipi: client di posta, browser web, ecc. Ogni tipo è caratterizzato da una serie di attività specifiche, come inviare e ricevere posta, o ricevere e visualizzare pagine html. Ogni tipo usa un determinato set di protocolli e porte di rete. È per questo che disporre di modelli per regole consente di effettuare una configurazione iniziale più facile e veloce delle regole in base al tipo di applicazione.

Per creare una regola per applicazioni da un modello:

1. Se non è già selezionata, selezionare la casella **Raggruppa regole per applicazione** nella scheda **Regole per applicazioni**, e fare clic sul pulsante **Aggiungi**.
2. Apparirà un menu contestuale che porterà ad una finestra di selezione di file standard attraverso l'opzione **Sfoglia** oppure ad un elenco di applicazioni attive attraverso l'opzione **Applicazioni** per eseguire la selezione. Questa, a sua volta, aprirà una finestra delle regole per l'applicazione selezionata. Queste saranno mostrate nella parte superiore della finestra. In assenza di regole, la finestra appare vuota.
3. Fare clic su **Modello** nella finestra delle regole per l'applicazione e selezionare uno dei modelli per le regole dal menu contestuale (vedi Figura 49).

Consenti tutto è una regola che autorizza qualsiasi attività di rete per l'applicazione. **Blocca tutto** è una regola che blocca qualsiasi attività di rete per l'applicazione. Qualsiasi tentativo di stabilire una connessione di rete da parte dell'applicazione in questione sarà bloccato senza informare l'utente.

Altri modelli elencati nel menu contestuale creano regole tipiche per i programmi corrispondenti. Per esempio, il modello **Programma di posta elettronica** crea una serie di regole che autorizzano attività di rete standard per client di posta, come l'invio di messaggi.

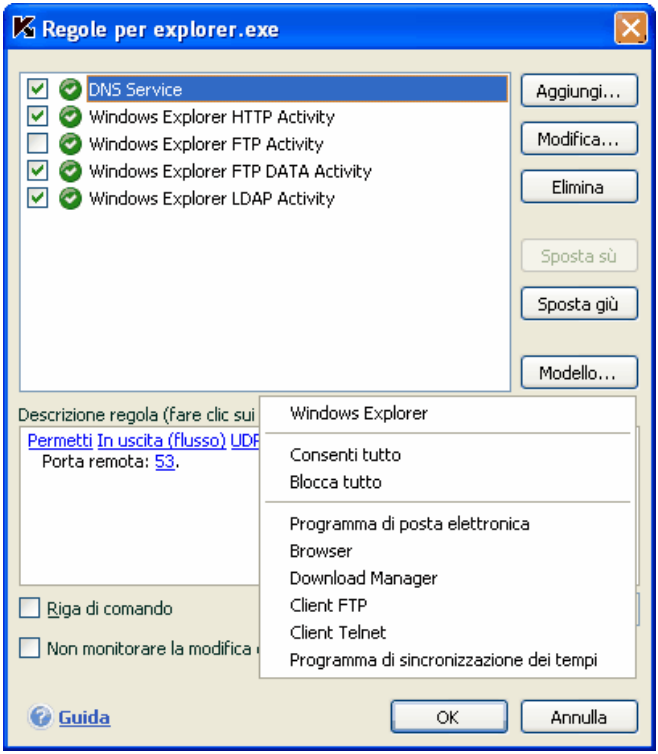


Figura 49. Selezione di un modello per la creazione di una nuova regola

4. Se necessario, modificare le regole create per l'applicazione. È possibile modificare azioni, direzione della connessione di rete, indirizzo remoto, porte (locale e remota) e l'intervallo temporale da assegnare alla regola.

5. Se si desidera applicare la regola a un'applicazione aperta con determinate impostazioni nella riga di comando, selezionare la casella **Riga di comando** e digitare la stringa nel campo a destra.

6. Affinché Firewall non controlli le modifiche ai file appartenenti all'applicazione controllata ogni volta che tenta di raggiungere la rete, selezionare **Non monitorare la modifica dei file dell'applicazione**.

La regola o serie di regole creata sarà aggiunta alla fine dell'elenco con la priorità più bassa. È possibile tuttavia aumentare la priorità della regola (vedi 12.1.1.5 pag. 172).

È possibile creare una regola dalla finestra di notifica di rilevamento di un'attività di rete (vedi 12.3 a pag. 185).

12.1.1.3. Regole di filtro pacchetti

Kaspersky Internet Security include una serie di regole utilizzate per filtrare i pacchetti di dati in arrivo e in uscita dal computer. Il trasferimento dei pacchetti dati può essere lanciato dall'utente stesso o da un'applicazione installata sul computer. Il programma include regole di filtro di pacchetti analizzate scrupolosamente dagli esperti Kaspersky Lab, che determinano se i pacchetti di dati sono pericolosi o attendibili.

A seconda del livello di sicurezza selezionato per il Firewall e del tipo di rete di cui fa parte di computer, l'elenco delle regole può essere utilizzato in vari modi. per esempio applicando solo regole di permesso con il livello di **Protezione alta**. I pacchetti non coperti da una regola di permesso vengono bloccati.

Attenzione!

Le regole per le zone di sicurezza hanno una priorità più elevata rispetto alle regole di blocco dei pacchetti. Quindi, se ad esempio si seleziona lo stato **Local Area Network,** lo scambio dei pacchetti sarà permesso così come l'accesso alle cartelle condivise indipendentemente dalle regole di blocco dei pacchetti.

Per lavorare con l'elenco delle regole di filtro pacchetti:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.

2. Cliccare su **Impostazioni** sotto **Sistema di filtro** (vedi Figura 47).

3. Selezionare la scheda **Regole per filtri pacchetti** nella finestra **Impostazioni: Firewall** (vedi Figura 52).

Per ogni regola di filtro pacchetti sono riportate le seguenti informazioni: nome della regola, azione (permesso o blocco del trasferimento del pacchetto),

protocollo di trasferimento dati, direzione del pacchetto e impostazioni della connessione di rete utilizzate per il trasferimento del pacchetto.

Se il nome della regola di filtro del pacchetto è selezionato, essa sarà applicata.

È possibile lavorare con l'elenco delle regole utilizzando i pulsanti a destra dell'elenco.

Per creare una nuova regola di filtro pacchetti:

Fare clic sul pulsante **Aggiungi** nella scheda **Regole per filtri pacchetti**.

Nella finestra **Nuova regola** che si apre è presente un modulo utilizzabile per mettere a punto una regola precisa (vedi 12.1.1.4 pag. 168).

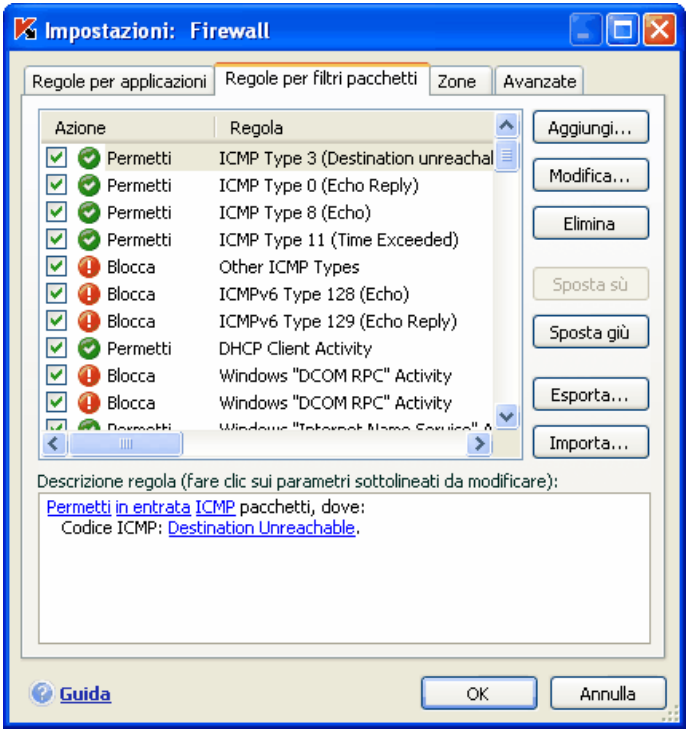


Figura 50. Elenco delle regole di filtro pacchetti

12.1.1.4. Messa a punto delle regole per applicazioni e filtro pacchetti

La finestra **Nuova regola** per le impostazioni avanzate delle regole è praticamente identica a quella per le applicazioni e il pacchetti di dati (vedi Figura 51).

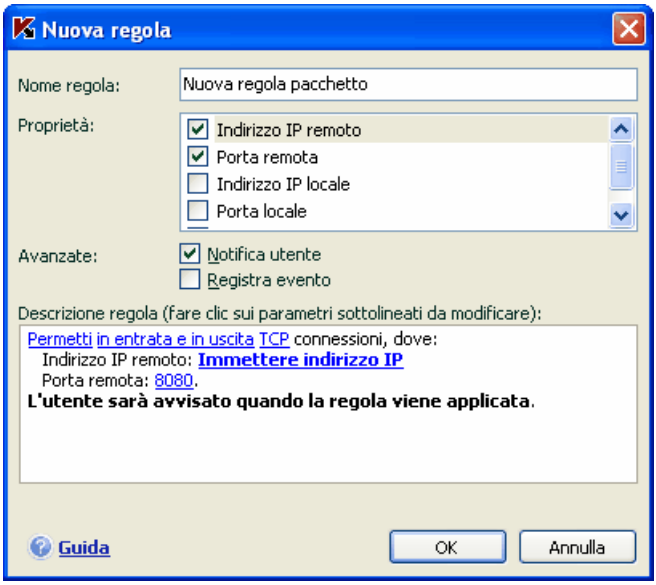


Figura 51. Creazione di una nuova regola per applicazioni

Passaggio 1:

- Digitare un nome per la regola. Il programma usa un nome predefinito che è possibile sostituire.
- Selezionare le impostazioni della connessione di rete per la regola: indirizzo remoto, porta remota, indirizzo locale, ora. Selezionare tutte le impostazioni che si desidera applicare alla regola.
- Configurare le altre impostazioni per le notifiche all'utente. Se si preferisce la visualizzazione di un pop-up con un breve commento ogni volta che si usa una regola, spuntare la casella **Notifica utente**. Se si desidera che il programma registri le informazioni relative all'applicazione della regola nel report del Firewall, selezionare la casella **Registra evento**. Per impostazione predefinita, al momento della creazione della regola la casella non è selezionata. Si

raccomanda di utilizzare le impostazioni avanzate durante la creazione di regole di blocco.

> Quando si crea una regola di blocco nella modalità apprendimento del Firewall, l'informazione circa la regola applicata verrà automaticamente riportata nel report. Se non occorre registrare questa informazione deselezionare **Registra evento** nelle impostazioni di quella regola.

Passaggio 2: assegnare dei valori ai parametri delle regole e selezionare le azioni. Queste operazioni si eseguono nella sezione **Descrizione regola**.

1. L'azione predefinita di ogni regola creata è *permetti*. Per modificare questa azione in una regola di blocco, fare clic con il pulsante sinistro del mouse sul link Permetti nella sezione della descrizione della regola. L'azione diventa Blocca.

   > Kaspersky Internet Security continuerà a scansionare il traffico di rete per i programmi e i pacchetti per i quali è stata creata una regola di permesso. Ciò potrebbe comportare una maggiore lentezza nel trasferimento dei dati.

2. Se non era stata selezionata un'applicazione prima di creare la regola, è necessario farlo adesso facendo clic su seleziona applicazione. Fare clic con il pulsante sinistro del mouse sul link e, nella finestra standard di selezione dei file che si apre, selezionare il file eseguibile dell'applicazione per la quale si sta creando la regola.

3. Quindi è necessario determinare la direzione della connessione di rete per la regola. Il valore predefinito è una regola per una connessione di rete bidirezionale. Per modificare la direzione, fare clic con il pulsante sinistro del mouse su in entrata e in uscita e selezionare la direzione della connessione di rete nella finestra che si apre:

   - **Flusso in entrata**. La regola si applica solo alle connessioni di rete aperte da un computer remoto che invia informazioni al computer dell'utente.
   - **Pacchetto in entrata**. La regola si applica a tutti i pacchetti dati ricevuti dal computer dell'utente, eccezion fatta per i pacchetti TCP.
   - **Flussi in Entrata ed Uscita**. La regola si applica al traffico in entrata e in uscita, indipendentemente dal computer (dell'utente o remoto) che ha avviato la connessione di rete.
   - **Flusso in uscita.** La regola si applica solo alle connessioni di rete aperte dal tuo computer.

Pacchetto in uscita. La regola si applica a tutti i pacchetti dati in entrata inviati dal computer dell'utente, eccezion fatta per i pacchetti TCP.

Se è importante impostare la direzione dei pacchetti specificamente nella regola, selezionare se si tratta di pacchetti in entrata o in uscita. Se si desidera creare una regola per il trasferimento dei dati in streaming, selezionare il flusso: in entrata, in uscita o entrambi.

La differenza tra la *direzione del flusso* e *direzione del pacchetto* è che quando si crea una regola per il flusso, si definisce la direzione in cui viene aperta la connessione. La direzione dei pacchetti durante il trasferimento dei dati su questa connessione non viene considerata.

Per esempio, se si configura una regola per lo scambio di dati con un server FTP in modalità passiva, è necessario autorizzare uno streaming (flusso) in uscita. Per scambiare dati con un server FTP in modalità attiva, si raccomanda di consentire i flussi sia in entrata che in uscita.

4. Se è stato selezionato un indirizzo IP remoto come proprietà di una connessione di rete, fare clic con il pulsante sinistro del mouse su immettere indirizzo IP e digitare l'indirizzo IP, una gamma di indirizzi o un indirizzo di sottorete nella finestra che si apre. È possibile usare uno o più tipi di indirizzo IP per una regola. Possono essere specificati più indirizzi per ciascun tipo.

   In una regola per pacchetti, può essere utilizzata una variabile ambientale di Windows al posto di un indirizzo IP.

5. Quindi è necessario impostare il protocollo usato dalla connessione di rete. TCP è il protocollo predefinito per la connessione. Se si sta creando una regola per applicazioni, è possibile selezionare il protocollo TCP o UDP facendo clic con il pulsante sinistro del mouse sul link con il nome del protocollo fino a visualizzare quello desiderato. Se si sta creando una regola per filtro pacchetti e si desidera modificare il protocollo predefinito, fare clic sul nome e selezionare il protocollo desiderato nella finestra che si apre. Se si seleziona ICMP, può essere necessario indicare il tipo.

6. Se sono state selezionate le impostazioni della connessione di rete (indirizzo, porta, intervallo temporale), è necessario assegnare loro anche dei valori esatti.

Dopo aver aggiunto la regola all'elenco di regole per l'applicazione, è possibile configurarla ulteriormente (vedi Figura 52):

- Se si intende applicare la regola all'applicazione aperta con determinate impostazioni nella riga di comando, selezionare **Riga di comando** e immettere la stringa nel campo a destra. La regola non sarà applicata alle applicazioni avviate con impostazioni diverse nella riga di comando.

- Affinché Firewall non controlli le modifiche ai file appartenenti all'applicazione controllata ogni volta che tenta di raggiungere la rete, selezionare ☑ **Non monitorare la modifica dei file dell'applicazione**.

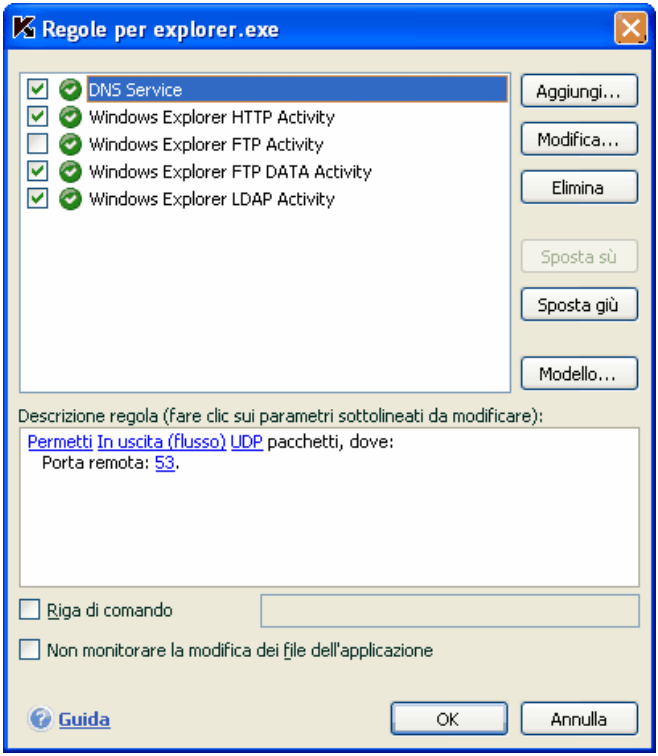


Figura 52. Impostazioni avanzate per nuova regola

Dopo aver aggiunto la regola all'elenco delle regole per applicazioni, è possibile configurarla ulteriormente (vedi Figura 52). Se si desidera applicare la regola a un'applicazione aperta con determinate impostazioni nella riga di comando, selezionare la casella ☑ **Riga di comando** e digitare la stringa nel campo a destra. Questa regola non sarà valida per le applicazioni avviate con una diversa riga di comando.

È possibile creare una regola dalla finestra di notifica del rilevamento di un'attività di rete (vedi 12.3 pag. 185).

12.1.1.5. Assegnazione della priorità alle regole

Ogni regola creata per un'applicazione o un pacchetto ha una determinata priorità. A parità di altre condizioni (per esempio le impostazioni della connessione di rete), l'azione applicata all'attività del programma sarà quella della regola con la priorità più elevata.

La priorità di una regola dipende dalla sua posizione nell'elenco delle regole. La prima regola dell'elenco è quella con la massima priorità. Ogni regola creata manualmente viene aggiunta all'inizio dell'elenco. Le regole create da modelli o da un avviso vengono aggiunte alla fine dell'elenco.

Per assegnare una priorità alle regole per applicazioni procedere come segue:

1. Selezionare il nome dell'applicazione nella scheda **Regole per applicazione** e cliccare su **Aggiungi**.
2. Usare i pulsanti **Sposta su** e **Sposta giù** nella finestra delle regole per applicazioni che si apre per spostare la posizione delle regole nell'elenco, modificando in tal modo l'ordine delle priorità.

Per assegnare una priorità alle regole di filtro pacchetti procedere come segue:

1. Selezionare la regola nella scheda **Regole per filtri pacchetti**.
2. Usare i pulsanti **Sposta su** e **Sposta giù** per spostare la posizione delle regole nell'elenco, modificando in tal modo la loro priorità.

12.1.1.6. Regole per zone di sicurezza

Dopo l'installazione, Firewall analizza l'ambiente di rete del computer. In base ai risultati dell'analisi, l'intero spazio di rete viene suddiviso in zone:

Internet – il World Wide Web. In questa zona, Kaspersky Internet Security agisce come un firewall personale. Così facendo, le regole predefinite di filtro pacchetti e delle applicazioni regolano l'intera attività di rete per garantire la massima sicurezza. Durante una sessione di lavoro in questa zona non è possibile modificare le impostazioni di protezione ma solo abilitare la modalità invisibile (Stealth) per una maggiore sicurezza del computer.

Zone di sicurezza – alcune zone, per lo più sottoreti alle quali appartiene il computer (per esempio sottoreti a casa o al lavoro). Per impostazione predefinita, queste zone sono definite "a medio rischio". È possibile modificare lo stato di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtro pacchetti e le applicazioni.

Se è abilitata la modalità Apprendimento del Firewall, si apre una finestra ogni volta che il computer si connette a una nuova zona, visualizzandone una breve descrizione. È necessario assegnare uno stato alla zona: in base ad esso l'attività di rete sarà autorizzata oppure no.

- **Internet**. È lo stato predefinito assegnato a Internet, poiché durante la navigazione il computer è soggetto a tutti i tipi di minacce potenziali. Questo stato è raccomandato anche per le reti non protette da programmi antivirus, firewall, filtri, ecc. Selezionando questo stato, il programma garantisce la massima sicurezza durante l'uso di questa zona, in particolare:
  - Blocco di qualsiasi attività di rete NetBios all'interno della sottorete.
  - Blocco delle regole per applicazioni e filtro pacchetti che consentono un'attività NetBios all'interno della sottorete.

  Anche se è stata creata una directory condivisa, le informazioni in essa contenute saranno disponibili solo agli utenti di sottoreti con questo stato. Inoltre, se per una data sottorete è selezionato questo stato, non è possibile accedere a file e stampanti di tale sottorete.
- **Rete locale**. Il programma assegna questo stato a tutte le zone rilevate durante l'analisi dell'ambiente di rete del computer, ad eccezione di Internet. Si raccomanda di applicare questo stato alle zone caratterizzate da un fattore di rischio medio (per esempio LAN aziendali). Selezionando questo stato, il programma consente:
  - Qualsiasi attività di rete NetBios all'interno della sottorete.
  - Regole per applicazioni e filtro pacchetti che consentono un'attività NetBios all'interno della sottorete.

  Selezionare questo stato se si desidera garantire l'accesso a determinate cartelle o stampanti del computer, bloccando al tempo stesso qualsiasi altra attività esterna.
- **Attendibile**. Questo stato è raccomandato solo per le zone ritenute assolutamente sicure, in cui il computer non è esposto ad attacchi o tentativi di accesso ai dati in esso custoditi. Se si seleziona questo stato, tutte le attività di rete sono consentite. Anche se in precedenza si è selezionato il massimo livello di protezione creando regole di blocco, questi sistemi di sicurezza non vengono applicati per i computer remoti provenienti da una zona attendibile.

Osservare che qualsiasi restrizione o autorizzazione all'accesso ai file ha valore solo all'esterno di questa sottorete.

Per una maggiore sicurezza durante l'uso di reti indicate come **Internet** è possibile attivare la *modalità invisibile*. Questa funzione consente solo le attività

di rete avviate dall'utente, in modo tale che il computer diventi invisibile all'ambiente circostante. Questa modalità non pregiudica le prestazioni del computer su Internet.

La modalità invisibile è sconsigliata se il computer funziona come server (per esempio un server di posta o HTTP). In tal caso infatti i computer che si connettono al server non riuscirebbero a vederlo come connesso.

L'elenco delle zone delle quali il computer fa parte è visualizzato nella scheda **Rete** (vedi Figura 53). Per ciascuna di esse sono indicati lo stato, una breve descrizione della rete e l'eventuale uso della modalità Stealth.

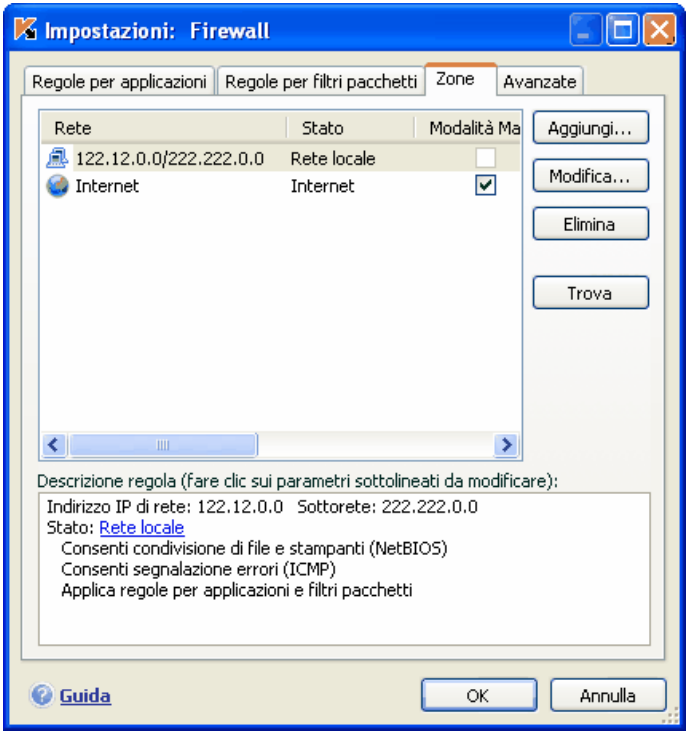


Figura 53. Elenco delle regole per le zone

Per modificare lo stato di una zona o abilitare/disabilitare la modalità invisibile, selezionarla dall'elenco e seguire i collegamenti appropriati nel riquadro **Descrizione regola** sotto l'elenco. È possibile eseguire attività simili e modificare indirizzi e maschere di sottoreti nella finestra **Impostazioni rete** che si apre facendo clic su **Modifica**.

È possibile aggiungere una nuova zona all'elenco durante la visualizzazione. A tal fine, fare clic su **Trova**. Firewall cerca le potenziali zone di registrazione, chiedendo eventualmente di selezionare uno stato da assegnare loro. È possibile inoltre aggiungere manualmente nuove zone all'elenco (per esempio se si connette il laptop a una nuova rete). Per fare questo, usare il pulsante **Aggiungi** e inserire le informazioni necessarie nella finestra **Impostazioni rete**.

Attenzione!

Le reti con campi di indirizzi simili o più ampi possono nascondere alter reti. Le reti nascoste possono essere solo a rilevamento automatico. Qualora una rete con un campo indirizzi più ampio compaia in elenco, tutte le reti nascoste aggiunte manualmente dall'utente saranno rimosse. Tutte le impostazioni configurate per la rete più ampia saranno ereditate dalle reti nascoste. Se viene rimossa una rete più ampia, le reti nascoste si separano e mantengono le impostazioni correnti.

Per eliminare una rete dall'elenco, fare clic sul pulsante **Elimina**.

12.1.1.7. Modalità Firewall

La modalità Firewall (vedi Figura 54) controlla la compatibilità di Firewall con i programmi che stabiliscono connessioni di rete multiple e con giochi in rete.

Compatibilità massima – Fornisce la compatibilità massima di Firewall con i programmi che stabiliscono connessioni di rete multiple, per esempio client di rete per la condivisione di file. Questa modalità tuttavia può comportare un rallentamento del tempo di reazione nei giochi in rete. In presenza di tali problemi si raccomanda di applicare la modalità **Alta velocità.**

Alta velocità – il Firewall garantisce un tempo di reazione ottimale durante i giochi in rete. Tuttavia questa opzione può provocare dei conflitti con client di condivisione file o altre applicazioni di rete. Per risolvere il problema disabilitare la modalità Stealth.

Per selezionare una modalità Firewall:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione.**
2. Cliccare su Impostazioni sotto **Abilita Sistema di filtro** (vedi Figura 47).
3. Selezionare la scheda **Avanzate** nella finestra **Impostazioni: Firewall** e configurare **Compatibilità massima** o **Alta velocità**.

Le modifiche alla modalità Firewall avranno effetto solo dopo aver riavviato il Firewall.

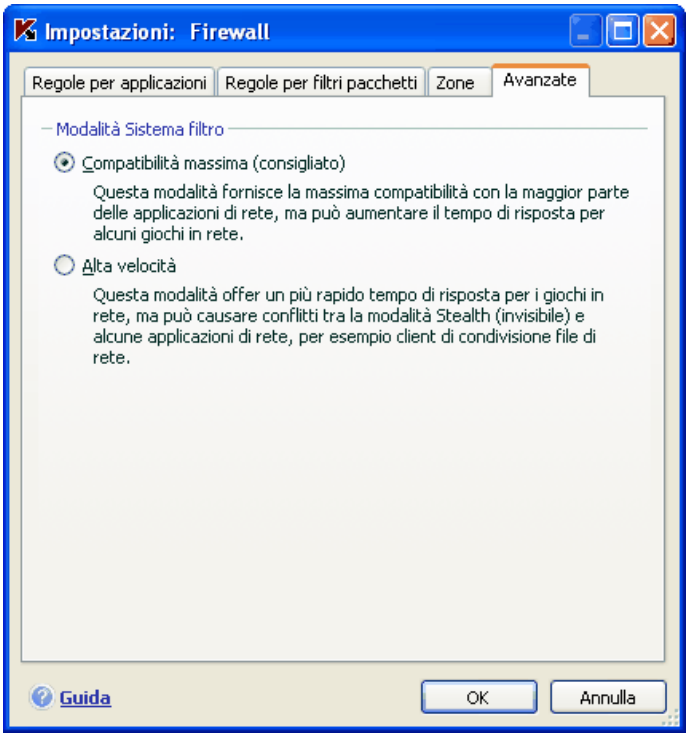


Figura 54. Selezione di una modalità Firewall

12.1.2. Sistema di rilevamento delle intrusioni

Tutti gli attacchi di rete noti che potrebbero mettere in pericolo il computer sono presenti nei database del Firewall che sono una sottorete dei database dell'applicazione. Questo elenco di attacchi è strettamente legato al modulo Sistema di rilevamento delle intrusioni del Firewall. L'elenco degli attacchi che il modulo è capace di riconoscere viene aggiornato durante l' aggiornamento del database (vedi Capitolo 16 pag. 244).

Il sistema di rilevamento delle intrusioni intercetta le attività di rete tipiche degli attacchi, e se intercetta un tentativo di attaccare il computer blocca qualsiasi attività di rete tra il computer remoto e quello dell'utente per un'ora. In questo caso viene visualizzato un messaggio che informa dell'avvenuto tentativo di attacco, con informazioni specifiche sul computer da cui l'attacco è partito.

È possibile configurare il sistema di rilevamento delle intrusioni procedendo come segue:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.
2. Spunta **Abilita Sistema di rilevamento intrusioni** e specificare se il computer dal quale proviene l'attacco deve essere aggiunto all'elenco delle applicazioni bloccate e per quanto tempo. Per impostazione predefinita, il computer dal quale proviene l'attacco verrà bloccato per 60 minuti. Questo tempo può essere aumentato o diminuito modificando il valore del campo posto accanto alla casella di spunta **Blocca computer da cui proviene l'attacco per ... min.** Deselezionare questa opzione se non si intende bloccare l'attività di rete del computer che ha tentato l'attacco.

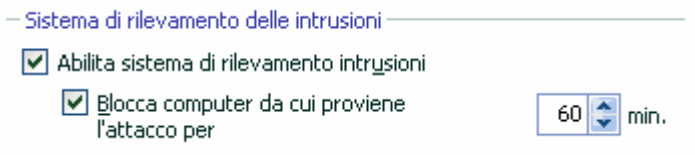


Figura 55. Configurazione del tempo di blocco per computer che tentano attacchi di rete

12.1.3. Anti-Pubblicità

Il modulo Anti-Pubblicità blocca l'accesso alle risorse Internet contenenti informazioni pubblicitarie come i pop-up.

I pop-up in genere non riportano informazioni utili. Queste finestre vengono aperte automaticamente quando un sito web è caricato per la prima volta o quando si esegue un collegamento ipertestuale. Esse contengono pubblicità o altre informazioni non richieste dall'utente. Anti-Pubblicità blocca queste finestre e mostra un messaggio speciale sopra l'icona dell'applicazione nell'area di notifica della barra delle applicazioni. Questo messaggio può essere utilizzato per bloccare o permettere il pop-up.

Anti-Pubblicità è compatibile con il popup blocker di Microsoft Internet Explorer fornito con Microsoft Windows XP Service Pack 2. L'applicazione installa un plugin che controlla l'apertura di finestre pop-up direttamente nel browser.

Ci sono alcuni siti che usano le finestre pop-up per una più efficiente navigazione. Se si accede a questi siti frequentemente, e le informazioni contenute in queste finestre sono importanti, consigliamo di aggiungere questi siti all'elenco dei siti attendibili. I pop-up dei siti attendibili non verranno bloccati.

Quando un pop-up viene bloccato durante una sessione di Microsoft Internet Explorer, l'icona viene mostrata nella riga di stato del browser. Cliccando sull'icona è possibile sbloccare il pop-up oppure aggiungere il sito all'elenco dei siti attendibili.

Per impostazione predefinita, il modulo Anti-Pubblicità blocca la maggior parte dei pop-up automatici. L'eccezione riguarda i pop-up dei siti web contenuti nell'elenco dei siti attendibili di Microsoft Internet Explorer e dei siti Intranet a cui il computer appartiene.

Nel sistema operativo Microsoft Windows XP con Service Pack 2, Internet Explorer già dispone di un proprio blocco pop-up che può essere configurato selezionando quali particolari finestre bloccare e quali altre no. Anti-Pubblicità è compatibile con questo blocker secondo il seguente principio: una regola di blocco ha la precedenza, vale a dire che se Internet Explorer o il modulo Controllo Privacy presentano una regola di blocco dei pop-up, la finestra verrà bloccata. Per tale ragione consigliamo di configurare insieme il browser ed il Popup Blocker se si opera su sistema operativo Microsoft Windows XP con Service Pack 2.

Se per qualsiasi ragione si desidera visualizzare un popup, occorre aggiungerla all'elenco degli indirizzi attendibili. A tal fine:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.
2. Spunta **Abilita Popup Blocker** sotto **Blocco Popup** e cliccare su **Siti Attendibili** (vedi Figura 46).
3. Cliccare su **Aggiungi** nella corrispondente finestra di dialogo **Impostazioni**: **URL attendibili** ed inserire la maschera dell'URL attendibile (vedi Figura 56).

> **Suggerimento:**
>
> Quando si immette la maschera di un indirizzo attendibile possono essere usati i caratteri * oppure ?.
>
> Ad esempio la maschera http://www.test* esclude i popup di ogni sito che inizia con questa serie di caratteri.

4. Specificare se gli indirizzi della zona attendibile di Internet Explorer o gli indirizzi della tua rete locale debbano essere esclusi dalla scansione. Il programma li considera attendibili per impostazione predefinita e non blocca i popup relativi a questi indirizzi.

La nuova esclusione verrà aggiunta in testa all'elenco degli indirizzi attendibili. Per interrompere l'uso dell'esclusione creata, deselezionare la casella vicino al suo nome. Per eliminare completamente una esclusione, selezionarla dall'elenco e cliccare su **Elimina**.

Per bloccare i popup della propria rete locale o dei siti web compresi nell'elenco dei siti attendibili di Microsoft Internet Explorer, deselezionare la corrispondente casella nella sezione **Area attendibile**.

Quando tentano di aprirsi dei popup di siti che non sono compresi nell'elenco dei siti attendibili, apparirà sull'icona del programma un messaggio che avverte di aver bloccato la finestra. Il messaggio contiene dei link che permettono di annullare il blocco ed aggiungere l'indirizzo della finestra all'elenco degli indirizzi attendibili.

Figura 56. Creazione elenco di indirizzi attendibili

È inoltre possibile sbloccare le finestre da Internet Explorer se si dispone di sistema operativo Microsoft Windows XP con Service Pack 2. A tal fine, utilizzare il menu contestuale che si apre sull'icona del programma che lampeggia nell'angolo inferiore del browser quando i popup vengono bloccati.

12.1.4. Anti-Banner

L'Anti-Banner blocca i messaggi pubblicitari posti in speciali banner online o inseriti nelle interfacce di numerosi programmi installati sul computer.

L'informazione contenuta nei banner pubblicitari non è utile. Essa distrae ed incrementa il traffico di rete. Anti Banner blocca i più comuni tipi di banner conosciuti al momento le cui descrizioni sono incluse in Kaspersky Internet Security sotto forma di normali espressioni. Il blocco dei banner può essere

disabilitato ed è possibile creare un elenco personalizzato di siti abilitati e disabilitati.

Per integrare Anti-Banner con il browser Opera, modificare la sezione **[Image Link Popup Menu]** di standard_menu.ini per aggiungere la seguente riga:

Item «New banner» = Copy image address & Execute program «<drive>\Program Files\Kaspersky Lab\Kaspersky Internet Security 7.0\opera_banner_deny.vbs» «//nologo %C».

Sostituire <drive> con il nome del proprio drive di sistema.

Un elenco di normali espressioni che descrivono i più comuni banner pubblicitari è stata creata dagli specialisti di Kaspersky Lab con studi particolareggiati ed è inclusa nel pacchetto. I banner pubblicitari che corrispondono alle espressioni dell'elenco verranno bloccati dall'applicazione a meno che il blocco sia disabilitato.

Inoltre, possono essere creati elenchi degli indirizzi consentiti e bloccati per gestire se i banner possono essere visualizzati o bloccati.

Notare che se una maschera di dominio è compresa nell'elenco dei banner bloccati o consentiti, l'accesso al sito web principale non è bloccato.

Per esempio se truehits.net è compreso nell'elenco dei banner bloccati, l'accesso a http://truehits.net sarà permesso mentre l'accesso a http://truehits.net/a.jpg verrà bloccato.

12.1.4.1. Configurazione dell'elenco standard dei banner pubblicitari bloccati

Kaspersky Internet Security comprende un elenco di maschere dei più comuni banner pubblicitari sui siti web e sulle interfacce dei programmi. Questo elenco è compilato dagli specialisti di Kaspersky Lab ed è aggiornato insieme ai database dell'applicazione.

È possibile selezionare quale maschera standard di banner pubblicitario usare per Anti-Banner. A tal fine:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.
2. Spuntare **Abilita Anti-banner** sotto **Blocco Banner Pubblicitari** e cliccare su **Impostazioni** (vedi Figura 46).
3. Aprire la scheda **Generale** nella finestra di dialogo **Impostazioni**: **Blocco dei banner** (vedi Figura 57). I caratteri jolly possono essere

utilizzati in qualsiasi punto dell'indirizzo di un banner. L'elenco delle maschere bloccate standard non può essere modificato.

Per non bloccare un banner coperto dall'elenco standard dei banner bloccati, deselezionare la casella corrispondente. Per analizzare i banner pubblicitari che non corrispondono alle maschere dell'elenco standard, **Utilizzare l'analizzatore euristico**. Così facendo, l'applicazione analizzerà le immagini caricate ricercando la presenza di segni tipici dei banner p'bblicitari. In seguito a questa analisi, l'immagine può essere identificata come un banner e bloccata.

È inoltre possibile creare un elenco di banner pubblicitari consentiti e bloccati, utilizzando le schede **Elenco consentiti** ed **Elenco bloccati**.

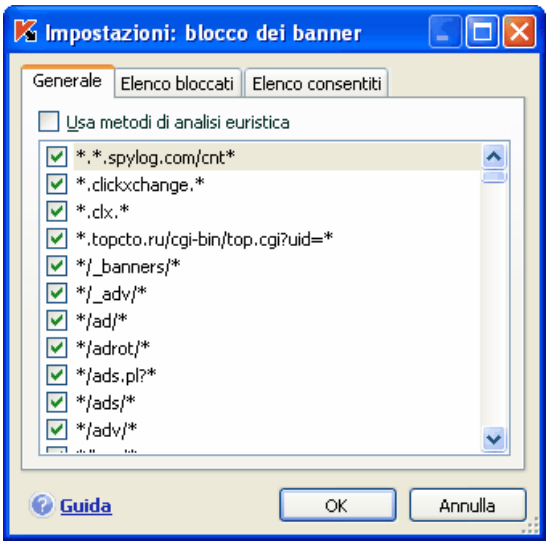


Figura 57. Elenco banner bloccati

12.1.4.2. Elenco Banner Pubblicitari Bianchi

Puoi creare un elenco di banner pubblicitari bianchi per permettere a certi banner di essere visti. Questo elenco contiene le maschere dei banner abilitati.

È possibile selezionare quale maschera standard di banner pubblicitario usare per Anti-Banner. A tal fine:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.
2. Spuntare **Abilita Anti-banner** sotto **Blocco Banner Pubblicitari** e cliccare su **Impostazioni** (vedi Figura 46).

3. Apri la **Lista Bianca** nella finestra di dialogo **Impostazioni**: **Blocco Banner**.

Utilizzando una finestra accessibile facendo clic sul pulsante **Aggiungi**, immettere una maschera per il banner che deve essere bloccato da Anti-Banner. È possibile specificare l'intero URL del banner o una maschera per lo stesso. In quest'ultimo caso, quando un banner tenta di caricarsi, il programma scansionerà il suo indirizzo alla ricerca della maschera.

Per la creazione di una maschera, si possono usare i caratteri jolly ***** o **?** (dove * rappresenta una sequenza di caratteri e ? qualsiasi carattere).

Per sospendere l'uso di una maschera creata, è possibile eliminarla dall'elenco o deselezionare la casella accanto alla stessa ☑.

I pulsanti **Importa** ed **Esporta** consentono di copiare l'elenco dei banner bloccati da un computer all'altro.

12.1.4.3. Elenco Banner Pubblicitari Bloccati

Oltre all'elenco standard dei banner bloccati (vedi 12.1.4.1 a pag. 180), possibile creare un elenco personalizzato. A tal fine:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Firewall** sotto **Protezione**.
2. Spuntare ☑ **Abilita Anti-banner** sotto **Blocco Banner Pubblicitari** e cliccare su **Impostazioni** (vedi Figura 46).
3. Apri la **Lista Nera** nella finestra di dialogo **Impostazioni**: **Blocco Banner**.

Utilizzando una finestra accessibile facendo clic sul pulsante **Aggiungi**, immettere una maschera per il banner che deve essere bloccato da Anti-Banner. È possibile specificare l'intero URL del banner o una maschera per lo stesso. In quest'ultimo caso, quando un banner tenta di caricarsi, il programma scansionerà il suo indirizzo alla ricerca della maschera.

Per la creazione di una maschera, si possono usare i caratteri jolly ***** o **?** (dove * rappresenta una sequenza di caratteri e ? qualsiasi carattere).

Per sospendere l'utilizzo di una maschera creata dall'utente, и possibile liminarla dall'elenco o deselezionare la casella ☑ di spunta corrispondente.

I pulsanti **Importa** ed **Esporta** consentono di copiare l'elenco dei banner bloccati da un computer all'altro.

12.2. Elenco degli attacchi di rete intercettati

Nota

La presente sezione fornisce informazioni generali sui tipi di attacchi di rete più diffusi e le loro potenziali conseguenze. Un elenco degli attacchi attivi rilevati direttamente dal componente Firewall può essere modificato dagli esperti di Kaspersky Lab in funzione della situazione corrente e può essere aggiornato con i database dell'applicazione.

Esistono attualmente numerosi attacchi di rete che sfruttano le vulnerabilità dei sistemi operativi e di altri software, sistemi o altro, installati sul computer. I pirati informatici sviluppano costantemente nuovi metodi di attacco, imparando come trafugare informazioni confidenziali, provocando anomalie di funzionamento del sistema o "impadronendosi" del computer per utilizzarlo come elemento di una rete fantasma da cui lanciare nuovi attacchi.

Per garantire la sicurezza del computer, è necessario conoscere i tipi di attacchi di rete possibili. Gli attacchi di rete noti possono essere suddivisi in tre categorie principali:

- **Scansione di porte** – questa minaccia non costituisce di per sé un attacco, ma di solito ne precede uno poiché si tratta di uno dei metodi più comuni per ottenere informazioni su un computer remoto. Le porte UDP/TCP utilizzate dagli strumenti di rete sull'indirizzo in questione vengono scansionate per capire se sono chiuse o aperte.

  Dalla scansione delle porte, un pirata è in grado di capire quali tipi di attacco funzioneranno sul sistema e quali no. Inoltre, le informazioni ottenute dalla scansione consentono di identificare il sistema operativo utilizzato dal computer remoto. Questo, a sua volta, circoscrive ulteriormente il numero degli attacchi possibili e, di conseguenza, il tempo necessario a lanciarli. Inoltre consente al pirata di sfruttare le vulnerabilità specifiche del sistema operativo.

- **Attacchi DoS (Denial of Service)** – si tratta di attacchi volti a rendere instabile o completamente inoperativo il sistema. Le conseguenze di questi attacchi sono il danneggiamento o la corruzione delle risorse dati a cui sono rivolti e l'impossibilità di utilizzare quelle risorse.

  Esistono due tipi principali di attacchi DoS:

  - L'invio al computer attaccato di pacchetti appositamente creati per provocare il riavvio o l'arresto del sistema.

- L'invio al computer attaccato di numerosi pacchetti in un lasso temporale estremamente breve che non consente al computer di elaborarli, esaurendo le risorse di sistema.

Quelli descritti di seguito sono esempi comuni di attacchi di questa categoria:

- *Ping of death* – consiste nell'invio di un pacchetto ICMP di dimensioni superiori a quelle massime di 64 KB. Questo attacco è in grado di bloccare completamente alcuni sistemi operativi.
- *Land* – consiste nell'inviare a una porta aperta del computer una richiesta di connessione con se stessa. Il computer entra in un circolo vizioso che incrementa il carico sul processore e può provocare il blocco di alcuni sistemi operativi.
- *ICMP Flood* – consiste nell'invio di un numero elevato di pacchetti ICMP al computer attaccato. L'attacco costringe il computer a rispondere a ciascun pacchetto in entrata, sovraccaricando gravemente il processore.
- *SYN Flood* – consiste nell'invio di un numero elevato di query al computer per stabilire una falsa connessione. Il sistema riserva determinate risorse a ciascuna di queste connessioni, assorbendo totalmente le risorse disponibili. In conseguenza di questo attacco, il computer non reagisce più ad altri tentativi di connessione.

- **Intrusioni**, volte a impadronirsi del computer attaccato. Si tratta del tipo di attacco più pericoloso di tutti poiché, se portato a buon fine, offre al pirata il controllo completo del computer.

  I pirati utilizzano questo tipo di attacco per ottenere informazioni confidenziali da un computer remoto (per esempio, numeri di carte di credito o password) o per controllare il sistema al fine di utilizzarne in seguito le risorse per fini illeciti (il sistema catturato sarà usato come elemento di reti fantasma o come piattaforma per nuovi attacchi).

  Questo gruppo comprende più attacchi di qualsiasi altro. Essi possono essere suddivisi in tre sottogruppi a seconda del sistema operativo: attacchi a Microsoft Windows, attacchi a Unix e attacchi efficaci con entrambi i sistemi operativi.

  I tipi di attacco più comuni che utilizzano strumenti del sistema operativo sono:

  - *Attacchi di overflow del buffer* – tipo di vulnerabilità del software che si manifesta a causa del controllo insufficiente o assente sulla gestione di massicci quantitativi di dati. È uno dei primi tipi di vulnerabilità scoperti dai pirati e il più facile da sfruttare.

- *Attacchi di stringhe di formato* – tipo di vulnerabilità che deriva da un controllo insufficiente dei valori di input per le funzioni I/O, quali printf(), fprintf(), scanf() e altri della libreria C standard. Se un programma presenta questa vulnerabilità, un pirata può ottenere il controllo completo del sistema servendosi di query create con una tecnica speciale.

Intrusion Detector analizza e blocca automaticamente i tentativi di sfruttare queste vulnerabilità dei più comuni strumenti di rete (FTP, POP3, IMAP) eseguiti sul computer dell'utente.

Gli *attacchi a Microsoft Windows* si basano sullo sfruttamento delle vulnerabilità dei software installati sul computer (per esempio, di programmi come Microsoft SQL Server, Microsoft Internet Explorer, Messenger e di componenti del sistema accessibili attraverso la rete come DCom, SMB, Wins, LSASS, IIS5).

Esistono inoltre isolati episodi di attacchi invasivi che utilizzano vari script nocivi, tra cui gli script elaborati da Microsoft Internet Explorer e da worm del tipo Helkern. Questi attacchi consistono in sostanza nell'invio di uno speciale tipo di pacchetti UDP a un computer remoto che può eseguire il codice nocivo.

Notare che, mentre si è connessi alla rete, il computer è costantemente a rischio di essere attaccato da un hacker. Per garantire la sicurezza del computer, abilitare il componente Firewall durante la navigazione in Internet e aggiornare regolarmente i database dell'applicazione (vedi 17.3.2 a pag. 255).

12.3. Blocco e autorizzazione di attività di rete

Se il livello di sicurezza del firewall è impostato su **Modalità apprendimento**, ogni volta che viene tentata una connessione di rete priva di regole viene visualizzato un apposito messaggio.

Per esempio, se il client di posta utilizzato è MS Outlook, esso scarica la posta da un Exchange server remoto. Per visualizzare la casella di posta in arrivo, il programma si connette al server di posta. Firewall intercetta sempre questo tipo di attività di rete e visualizza un messaggio (vedi Figura) contenente:

- *La descrizione dell'attività* – il nome dell'applicazione e le caratteristiche della connessione che sta avviando. Generalmente vengono indicati anche il tipo di connessione, la porta locale da cui è avviata, la porta remota e l'indirizzo a cui ci si connette. Fare clic con il pulsante sinistro del mouse su un punto qualsiasi del messaggio per ottenere

informazioni più dettagliate sull'attività di rete. La finestra che si apre contiene informazioni sulla connessione, sul processo che l'ha iniziata e sullo sviluppatore dell'applicazione.

- *L'azione* – le operazioni che il Firewall eseguirà relative all'attività di rete rilevata.

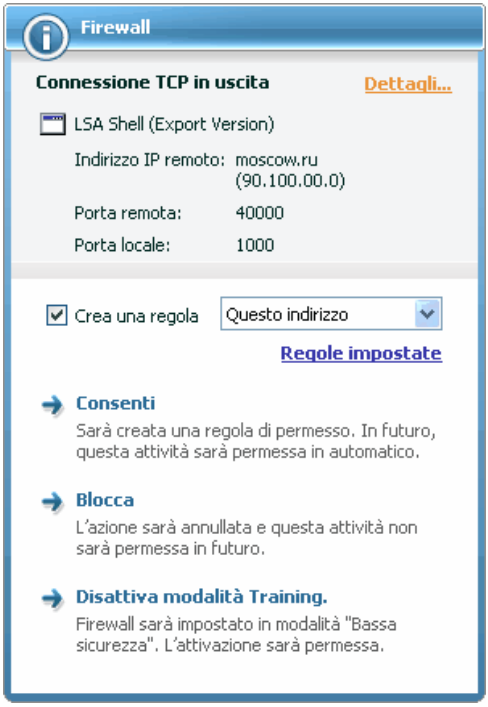


Figura 58. Notifica di attività di rete

Consultare con attenzione le informazioni sull'attività di rete e solo dopo selezionare le azioni del Firewall. Si raccomanda di decidere tenendo conto dei seguenti suggerimenti:

1. Prima di procedere, stabilire se permettere o bloccare l'attività di rete. È possibile che nella situazione specifica una serie di regole già create per l'applicazione o pacchetto possa essere di aiuto (supponendo che sia stata creata). A tal fine, utilizzare il collegamento Modifica regole. Si apre quindi una finestra contenente un elenco completo delle regole create per l'applicazione o pacchetto dati.
2. Decidere quindi se eseguire l'azione una sola volta o automaticamente ogni volta che viene intercettata questa attività.

Per eseguire l'azione una sola volta:

Deselezionare la casella **Crea una regola** e fare clic sul pulsante con il nome dell'azione, Permetti o Blocca.

Per eseguire automaticamente l'azione selezionata ogni volta che questa attività viene iniziata sul computer:

1. Selezionare la casella **Crea una regola**.
2. Selezionare il tipo di attività che si desidera eseguire dall'elenco a discesa:
   - **Tutte le attività** – qualsiasi attività di rete iniziata dall'applicazione.
   - **Personalizzato** – attività specifiche che l'utente dovrà definire in un'apposita finestra come per la creazione di una regola (vedi 12.1.1.2.1 pag. 164).
   - **<Modello>** – il nome del modello che include la serie di regole tipiche dell'attività di rete dell'applicazione. Questo tipo di attività è incluso nell'elenco se Kaspersky Internet Security possiede un modello appropriato per l'applicazione che ha iniziato l'attività di rete (vedi 12.1.1.2.2 pag. 164). In tal caso non è necessario personalizzare le attività da permettere o da bloccare. È sufficiente usare il modello per creare automaticamente una serie di regole per l'applicazione.
3. Fare clic sul pulsante con il nome dell'azione Permetti o Blocca.

Ricordare che la regola creata sarà usata solo quando tutti i parametri della connessione corrispondono a quelli indicati. Per esempio, questa regola non viene applicata a connessioni stabilite da una porta locale diversa.

Per disattivare i messaggi del Firewall mostrati per ogni applicazione che tenta di stabilire una connessione cliccare Disabilita Modalità Apprendimento. Questo metterà il Firewall nella modalità Tutte le Attività che consente tutte le connessioni eccetto quelle specificate esplicitamente dalle regole.

CAPITOLO 13. PROTEZIONE SPAM

Kaspersky Internet Security 7.0 include uno speciale componente che intercetta lo spam e lo elabora in base alle regole del client di posta, consentendo all'utente di risparmiare tempo durante l'uso della posta elettronica.

La posta elettronica viene sottoposta a scansione antispam in base al seguente metodo:

1. L'indirizzo del mittente viene confrontato con l'elenco Consentiti e Bloccati degli indirizzi.
    - Se è presente nell'Elenco consentiti, il messaggio viene classificato come *Non spam*.
    - Se è presente nell'Elenco bloccati, il messaggio viene classificato come *Spam*. Ulteriori analisi dipendono dall'azione selezionata (vedi 13.3.7 a pag. 207).
2. Se l'indirizzo del mittente non è presente né nell'Elenco consentiti, né nell'Elenco bloccati, il messaggio viene analizzato per mezzo della tecnologia PDB (vedi 13.3.2 a pag. 197).
3. Anti-Spam esamina in dettaglio il testo del messaggio e cerca frasi presenti nell'Elenco bloccati o Elenco consentiti.
    - Se il testo contiene frasi presenti nella sezione Frasi consentite dell'Elenco consentiti, il messaggio è classificato come *Non spam*.
    - In presenza di frasi contenute nell'Elenco frasi bloccate dell'Elenco bloccati, il messaggio è classificato come *spam*. L'ulteriore elaborazione dipende dall'azione selezionata.
4. Se il messaggio non contiene frasi presenti né nell'elenco delle frasi consentite né in quello delle frasi bloccate, viene sottoposto a scansione anti-phishing. Se il testo contiene un indirizzo presente nel database anti-phishing, il messaggio è classificato come *spam*. L'ulteriore elaborazione dipende dall'azione selezionata.
5. Se il messaggio non contiene elementi di phishing, viene sottoposto a scansione antispam utilizzando speciali tecnologie:
    - Analisi grafica mediante tecnologia GSG.
    - Analisi del testo mediante l'algoritmo di Bayes per il riconoscimento dello spam.

6. Quindi il messaggio viene scansionato alla ricerca di fattori di filtro spam avanzati (vedi 13.3.5 a pag. 205) impostati dall'utente al momento dell'installazione di Anti-Spam. Questa fase potrebbe includere l'analisi dei tag HTML, delle dimensioni dei caratteri o degli eventuali caratteri nascosti.

Ciascuna di queste fasi dell'analisi può essere disabilitata o abilitata.

Sono disponibili plug-in Anti-Spam per i seguenti client di posta:

- Microsoft Office Outlook (vedi 13.3.8 a pag. 208).
- Microsoft Outlook Express (vedi 13.3.9 a pag. 211).
- The Bat! (vedi 13.3.10 a pag. 213).

La barra delle applicazioni di Microsoft Outlook e Microsoft Outlook Express presenta due pulsanti, **Spam** e **Non Spam**, che consentono di configurare Anti-Spam in modo da individuare lo spam direttamente nella casella della posta. Questi pulsanti non sono presenti in The Bat!, ma il programma può essere addestrato utilizzando gli speciali elementi **Segna come spam** e **Segna come NON spam** nel menu **Speciale**. Inoltre, alle impostazioni del client di posta vengono aggiunti speciali parametri di elaborazione antispam (vedi 13.3.1 a pag. 196).

Anti-Spam fa uso di un algoritmo di Bayes modificato per l'autoapprendimento, che consente al componente di imparare a distinguere tra *spam* e *non spam*. L'algoritmo preleva i dati dal contenuto della lettera.

Si presentano situazioni in cui l'algoritmo di Bayes modificato per l'autoapprendimento non è in grado di classificare un determinato messaggio come spam o non spam con precisione. Questi messaggi vengono classificati come *probabile spam*.

Per ridurre il numero di messaggi classificati come probabile spam, si raccomanda di effettuare l'ulteriore apprendimento Anti-Spam (vedi 13.2 a pag. 191) per tali messaggi, specificando quali di essi devono essere classificati come *spam* e quali come *non spam*.

I messaggi riconosciuti come *spam* o *probabile spam* vengono modificati: alla riga dell'oggetto vengono aggiunte le annotazioni **[!! SPAM]** o **[?? Probable spam]**.

Le regole per l'elaborazione dei messaggi classificati come spam o probabile spam in MS Outlook, Outlook Express o The Bat! possono essere configurate in speciali plug-in creati appositamente per questi client. Per altri client di posta, è possibile creare delle regole di filtro che prendano in considerazione la riga dell'oggetto e, per esempio, configurarli in modo da spostare i messaggi in cartelle apposite a seconda che contengano **[!! SPAM]** o **[?? Probable spam]**. Per una descrizione più dettagliata del meccanismo di filtro, consultare la documentazione del client di posta usato.

13.1. Selezione di un livello di sensibilità per Anti-Spam

Kaspersky Internet Security protegge il computer dallo spam in base a uno dei seguenti livelli (vedi Figura 59):

Blocca tutto – il livello di sensibilità più severo, che classifica come spam tutti i messaggi che non contengono frasi presenti nelle Frasi consentite (vedi 13.3.4.1 a pag. 200) e i cui mittenti non sono elencati nei Mittenti consentiti dell'Elenco consentiti. A questo livello, i messaggi vengono esaminati confrontandoli con l'Elenco consentiti. Tutte le altre funzioni sono disabilitate.

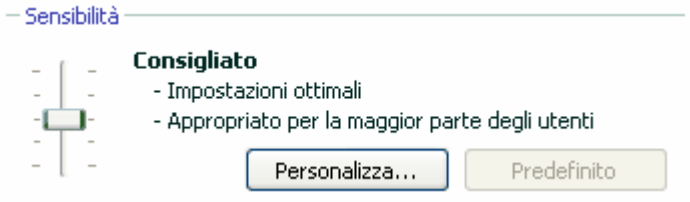


Figura 59. Selezione di un livello di sicurezza per Anti-Spam

Alta – un livello severo che, se attivato, aumenta la probabilità che alcuni messaggi effettivamente non spam vengano classificati come *spam*. A questo livello, il messaggio viene esaminato a fronte dell'Elenco consentiti ed Elenco bloccati, mediante le tecnologie PDB e GSG e in base all'algoritmo di Bayes (vedi 13.3.2 a pag. 197).

Questo livello deve essere adottato solo nei casi in cui la probabilità che l'indirizzo del destinatario sia ignoto agli spammer è elevata, per esempio quando il destinatario non è iscritto a nessuna mailing list e non possiede un indirizzo e-mail su server gratuiti/non aziendali.

Consigliato – il livello standard per classificare i messaggi.

A questo livello è possibile che alcuni messaggi spam non siano intercettati, segnalando così un apprendimento di Anti-Spam insufficiente. Si raccomanda di effettuare l'apprendimento supplementare del modulo utilizzando l'apprendimento guidato (vedi 13.2.1 a pag. 192) o il pulsante **Spam/NON Spam** (o voci di menu corrispondenti in The Bat!) per i messaggi classificati in maniera erronea.

Bassa – il livello più permissivo. Può essere raccomandato per gli utenti la cui corrispondenza, per qualsiasi motivo, contiene un numero significativo di parole riconosciute come spam da Anti-Spam, senza essere tali. Ciò può

essere dovuto all'attività professionale del destinatario, che richiede per la corrispondenza con i colleghi l'uso di un linguaggio ampiamente diffuso tra gli spammer. Tutte le tecnologie di intercettazione dello spam sono utilizzate per analizzare i messaggi a questo livello.

Consenti tutti – il livello di sicurezza più basso. A questo livello sono riconosciuti come spam solo i messaggi che contengono frasi presenti nella sezione Frasi bloccate e Mittenti bloccati della scheda Elenco bloccati. I messaggi vengono esaminati solo a fronte dell'Elenco bloccati. Tutte le altre funzioni sono disabilitate.

Per impostazione predefinita, la protezione antispam è impostata sul livello **Consigliato**. È possibile tuttavia aumentare o ridurre il livello di protezione oppure modificare le impostazioni del livello corrente.

Per modificare il livello di sensibilità:

Nella scheda **Riconoscimento spam** delle impostazioni avanzate del **Livello di protezione**, spostare il cursore verso destra o verso sinistra fino all'impostazione desiderata. Regolando il livello di sensibilità si definisce la correlazione tra i fattori di spam, probabile spam e messaggi accettati (vedi 13.3.3 a pag. 198).

Per modificare le impostazioni del livello di sensibilità corrente:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Anti-Spam** sotto **Protezione**.
2. Fare clic su **Personalizza** e poi aprire la scheda **Riconoscimento spam** (vedi Figura 59).
3. Modificare i parametri all'interno della finestra e fare clic su **Ok**.

A questo punto il livello di sensibilità sarà personalizzato.

13.2. Addestramento di Anti-Spam

Anti-Spam è dotato di un database di posta preinstallato contenente cinquanta esempi di spam. Si raccomanda tuttavia di sottoporre il modulo Anti-Spam a un ulteriore addestramento basato sui messaggi ricevuti.

Esistono diversi approcci di addestramento di Anti-Spam:

- Usare la Procedura guidata di apprendimento (vedi 13.2.1 a pag. 192).
- Addestrare Anti-Spam (vedi 13.2.2 a pag. 193) in base alle e-mail inviate.

- Addestrare il programma direttamente mentre si lavora con la posta elettronica (vedi 13.2.4 a pag. 194) utilizzando gli appositi pulsanti nel pannello strumenti o nei menu del client.
- Addestrare Anti-Spam con i report (vedi 13.2.4 a pag. 194).

L'addestramento mediante procedura guidata è il migliore fin dal primo utilizzo di Anti-Spam. La procedura guidata è in grado di addestrare Anti-Spam in base a un numero molto elevato di messaggi.

Osservare che non è possibile addestrare Anti-Spam con più di 50 messaggi per cartella. In presenza di cartelle contenenti un numero superiore di messaggi, il programma ne utilizzerà solo 50 ai fini dell'addestramento.

Il training supplementare utilizzando gli speciali pulsanti nell'interfaccia del client è preferibile quando si sceglie di lavorare direttamente sui messaggi.

13.2.1. Procedura guidata di apprendimento

La Procedura guidata di apprendimento consente di addestrare Anti-Spam indicando le cartelle di posta che contengono spam e messaggi accettabili.

Per avviare la Procedura guidata di apprendimento:

Selezionare **Anti-Spam** nella sezione **Protezione** nella parte sinistra della schermata principale e fare clic su **Apprendimento guidato**.

Anche la finestra delle impostazioni dell'applicazione può essere usata per iniziare l'apprendimento di Anti-Spam. Selezionare **Anti-Spam** nella sezione **Protezione** e fare clic su **Apprendimento guidato** nell'area **Apprendimento**.

La Procedura guidata di apprendimento guida l'utente passo passo nell'addestramento di Anti-Spam. Facendo clic sul pulsante **Avanti** si apre la fase successiva dell'addestramento, mentre il pulsante **Indietro** consente di tornare alla fase precedente.

La passagio 1 della Procedura guidata di apprendimento richiede la selezione delle cartelle contenenti la posta accettabile. In questa fase è sufficiente selezionare le cartelle i cui contenuti sono ritenuti assolutamente attendibili.

La passagio 2 della Procedura guidata di apprendimento consiste nella selezione delle cartelle contenenti lo spam.

Nella passagio 3 Anti-Spam viene addestrato automaticamente sulle cartelle selezionate. I messaggi presenti in queste cartelle costituiranno il database

di Anti-Spam. I mittenti dei messaggi accettabili vengono inseriti automaticamente nell'elenco consentiti dei mittenti.

Nella passagio 4 è necessario salvare i risultati dell'addestramento applicando uno dei seguenti metodi: Aggiungere i risultati dell'apprendimento al database corrente o sostituire il database corrente con i risultati dell'apprendimento. Ricordare che, affinché il meccanismo di intercettazione dello spam funzioni correttamente, è necessario addestrare il programma su un minimo di 50 messaggi accettabili e 50 messaggi di spam. In caso contrario l'algoritmo di Bayes non funzionerà.

Per risparmiare tempo, la Procedura guidata di apprendimento limita l'addestramento a 50 messaggi tra quelli presenti in ciascuna cartella selezionata.

13.2.2. Addestramento con i messaggi in uscita

È possibile addestrare Anti-Spam con i messaggi in uscita direttamente dal client di posta. L'elenco consentiti dei mittenti Anti-Spam viene integrata con gli indirizzi dei messaggi in uscita. Per l'apprendimento vengono utilizzati solo i primi 50 messaggi, dopodiché la procedura è completa.

Per addestrare Anti-Spam con i messaggi in uscita:

1. Selezionare **Anti-Spam** nella finestra **Protezione**.
2. Selezionare la casella ☑ **Apprendimento con i messaggi di posta in uscita** nella sezione **Apprendimento**.

Attenzione!

Se si seleziona la casella ☑ **Scansiona tutto-invio** del plug-in di Microsoft Outlook E-mail Anti-Virus (vedi 13.3.8 a pag. 208), Anti-Spam utilizza per l'addestramento solo i messaggi in uscita inviati tramite il protocollo MAPI.

13.2.3. Apprendimento mediante il client di posta

Per addestrare il programma direttamente dalla casella di posta, è possibile utilizzare gli appositi pulsanti sul pannello degli strumenti del client.

Al momento dell'installazione sul computer, Anti-Spam installa i plug-in dei seguenti client di posta:

- Microsoft Office Outlook
- Microsoft Outlook Express (Client di posta di Windows)
- The Bat!

Ad esempio nella barra degli strumenti di Microsoft Office Outlook ci sono due pulsanti, **Spam** e **Non spam**, e la scheda delle impostazioni di **Anti-Spam** (vedi 13.3.8 a pag. 208) nella finestra di dialogo **Opzioni** (voce di menu **Strumenti→ Opzioni**). Microsoft Outlook Express (Client di posta di Windows) in oltre ai pulsanti **Spam** e **Non spam** presenta anche il pulsante **Configura** sulla barra degli strumenti che apre una finestra con le azioni (vedi 13.3.9 a pag. 211) da compiere quando viene rilevato lo spam. In The Bat! questi pulsanti non ci sono, ma il programma può essere addestrato utilizzando le voci speciali **Segna come spam** e **Segna come NON spam** nel menu **Speciale**.

Se si decide di classificare come spam il messaggio selezionato, fare clic sul pulsante **Spam**. Se il messaggio non è da considerare spam, fare clic su **Non spam**. Anti-Spam esegue quindi il training sull'ultimo messaggio selezionato. Se si selezionano diversi messaggi, essi vengono tutti utilizzati per il training.

Attenzione!

Nei casi in cui si abbia necessità di selezionare immediatamente più messaggi, o si sia assolutamente certi che una determinata cartella contiene solo messaggi appartenenti a un unico gruppo (spam o non spam), è possibile adottare un approccio di apprendimento più complesso per mezzo della Procedura guidata di apprendimento (vedi 13.2.1 a pag. 192).

13.2.4. Apprendimento con i report di Anti-Spam

Esiste l'opzione di apprendimento di Anti-Spam attraverso i report.

Per visualizzare i report del componente:

1. Selezionare **Anti-Spam** nella sezione **Protezione** della finestra principale del programma.
2. Fare clic su **Apri Report**.

In base ai report del componente è possibile trarre conclusioni sull'accuratezza della configurazione e, se necessario, apportare determinate correzioni ad Anti-Spam.

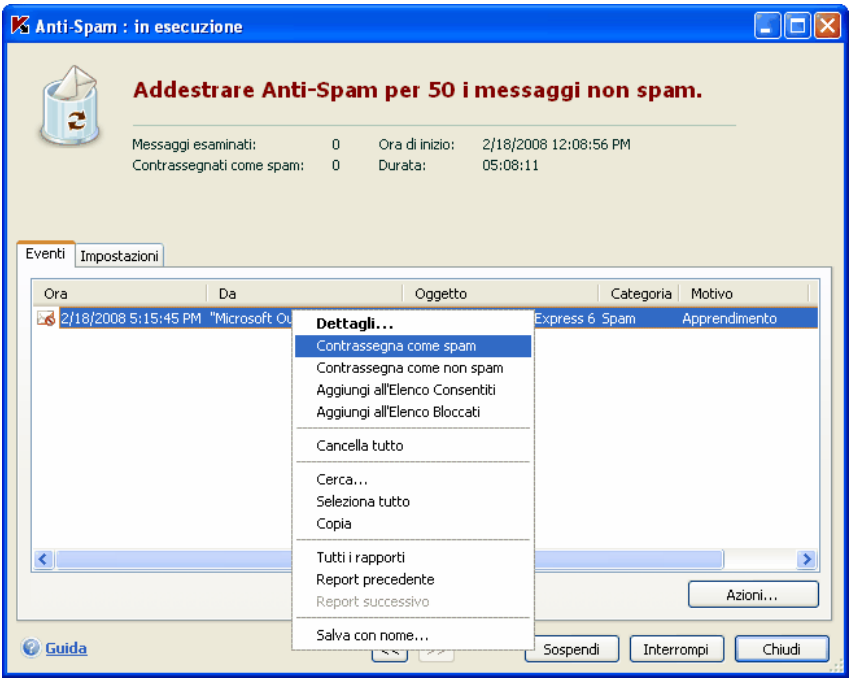


Figura 60. Addestramento di Anti-Spam dai report

Per classificare un determinato messaggio come spam o non spam:

1. Selezionare il messaggio dell'elenco dei report nella scheda **Eventi** e usare il pulsante **Azioni**.
2. Selezionare una delle quattro opzioni seguenti:
   - **Segna come spam**
   - **Segna come non spam**
   - **Aggiungi alla lista bianca**
   - **Aggiungi alla lista nera**

Anti-Spam esegue un ulteriore apprendimento sulla base di questo messaggio.

13.3. Configurazione di Anti-Spam

La configurazione di precisione di Anti-Spam è essenziale ai fini di un'efficace intercettazione dello spam. Tutte le impostazioni per il funzionamento del

componente si trovano nella finestra delle impostazioni di Kaspersky Internet Security e consentono di:

- Determinare i dettagli del funzionamento di Anti-Spam (vedi 13.3.1 a pag. 196).
- Scegliere quali tecnologie di filtro antispam utilizzare (vedi 13.3.2 a pag. 197).
- Regolare l'accuratezza di riconoscimento dello spam e del probabile spam (vedi 13.3.3 a pag. 198).
- Creare elenchi di mittenti e frasi ricorrenti consentiti e bloccati (vedi 13.3.4 a pag. 199).
- Configurare ulteriori funzioni di filtro antispam (vedi 13.3.5 a pag. 205).
- Ridurre al minimo la quantità di spam nella casella di posta in entrata grazie alla visualizzazione in anteprima con Mail Dispatcher (vedi 13.3.6 a pag. 206).

La presente sezione prende in esame queste impostazioni.

13.3.1. Configurazione delle impostazioni di scansione

È possibile configurare le seguenti impostazioni di scansione:

- Inclusione del traffico tramite protocolli POP3/IMAP nella scansione. Kaspersky Internet Security esamina per impostazione predefinita i messaggi trasferiti mediante tutti questi protocolli.
- Attivazione dei plug-in per MS Outlook, MS Outlook Express e The Bat!
- Visualizzazione dei messaggi mediante POP3 con Mail Dispatcher (vedi 13.3.6 a pag. 206) prima di scaricarla dal server di posta nella casella della posta in entrata dell'utente.

Per configurare le impostazioni sopra elencate:

1. Selezionare **Anti-Spam** nella finestra **Protezione**.
2. Selezionare o deselezionare le caselle nella sezione **Connettività** alle voci che corrispondono a quanto sopra elencato (vedi Figura 61).
3. Se necessario modificare le impostazioni di rete.

Attenzione!

Se il clienti d posta utilizzato è Microsoft Outlook Express, l'applicazione di posta elettronica deve essere riavviata ogni qualvolta lo stato dell'opzione **Abilita supporto per Microsoft Office Outlook, Outlook Express e The Bat!** Cambia.

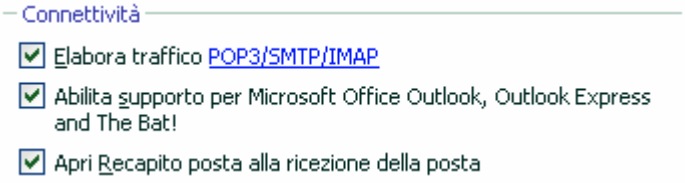


Figura 61. Configurazione delle impostazioni di scansione

13.3.2. Selezione delle tecnologie di filtro antispam

I messaggi vengono sottoposti alla scansione antispam mediante tecnologie di filtro all'avanguardia:

- **iBayes**, basata sul teorema di Bayes, analizza il testo dei messaggi per individuare frasi ricorrenti nello spam. L'analisi si basa sui dati statistici ottenuti mediante il training di Anti-Spam (vedi 13.2 a pag. 191).
- **GSG**, analizza gli elementi grafici nei messaggi per mezzo di speciali firme grafiche per individuare lo spam in formati non di testo.
- **PDB**, analizza le intestazioni dei messaggi e le classifica come spam sulla base di una serie di regole euristiche.
- **Recent Terms**, che esegue l'analisi del testo delle e-mail per identificare le frasi comunemente classificate come spam. L'analisi è condotta utilizzando i database utilizzati dagli esperti di Kaspersky Lab.

Per impostazione predefinita, tutte queste tecnologie di filtro sono abilitate, sottoponendo i messaggi a una scansione antispam più completa possibile.

Per disabilitare una o più tecnologie di filtro:

1. Aprire la finestra delle impostazioni di **Anti-Spam** nella sezione **Protezione**.
2. Fare clic su **Personalizza** nella sezione **Livello di protezione**, e nella finestra che si apre selezionare la scheda **Riconoscimento spam** (vedi Figura 62).

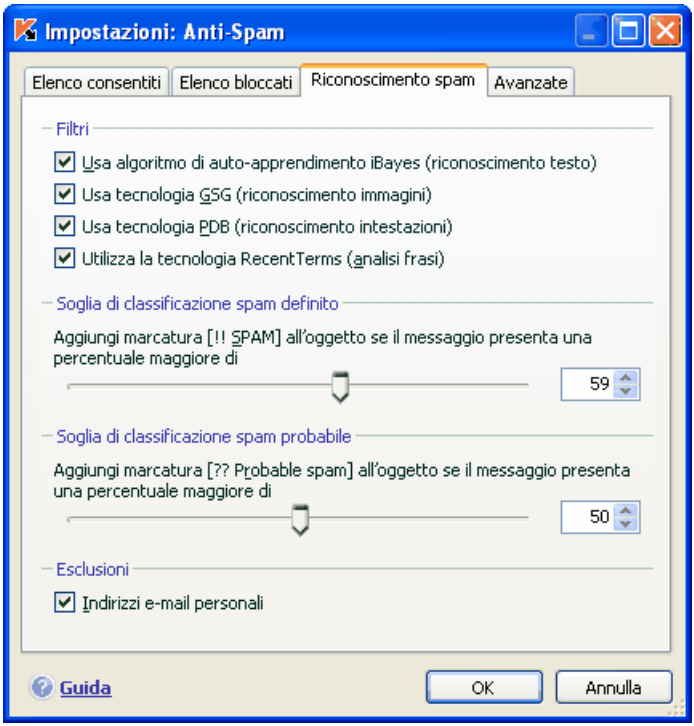


Figura 62. Configurazione del riconoscimento dello spam

3. Deselezionare le caselle a fianco delle tecnologie di filtro che non si desidera utilizzare ai fini del riconoscimento.

Per escludere il traffico e-mail (per esempio la posta aziendale) dall'analisi anti-spam, selezionare **Non controllare i messaggi nativi di Microsoft Exchange Server**. Notare che i messaggi saranno considerati come posta interna se Microsoft Office Outlook è utilizzato come client di posta su tutta la rete e se le caselle di posta dell'utente si trovano su un solo Exchange server o su più server collegati con connettori X.400. Deselezionare l'opzione affinché Anti-Spam analizzi questi messaggi.

13.3.3. Definizione dei fattori di spam e probabile spam

Gli esperti Kaspersky Lab hanno configurato Anti-Spam in maniera ottimale per riconoscere lo spam e il probabile spam.

Il riconoscimento dello spam si basa su tecnologie di filtro all'avanguardia (vedi 13.3.2 a pag. 197) che addestrano Anti-Spam all'identificazione di spam, probabile spam e non spam con un elevato grado di precisione utilizzando un certo numero di messaggi presenti nella casella della posta in entrata.

L'addestramento di Anti-Spam può essere eseguito per mezzo della Procedura guidata di training oppure sulla base dei messaggi elaborati dai client di posta. Così facendo, ad ogni singolo elemento dei messaggi accettati o dello spam viene assegnato un fattore. Quando un messaggio entra nella casella dei messaggi in entrata, Anti-Spam lo esamina con iBayes cercando eventuali elementi di spam e di messaggi accettati. I fattori di ciascun elemento vengono sommati ottenendo un *fattore di spam* e un *fattore di non spam.*

Il fattore di probabile spam definisce la probabilità che il messaggio sia classificato come tale. Se si sta utilizzando il livello **Consigliato**, ogni messaggio è caratterizzato da una probabilità di essere considerato *probabile spam* compresa tra il 50% e il 59%. La posta che, in seguito alla scansione, ottiene una probabilità inferiore al 50% viene considerata non spam.

Il fattore di spam determina la probabilità che Anti-Spam classifichi un messaggio come spam. Qualsiasi messaggio con probabilità superiori a quella sopra indicata saranno classificate come spam. Per impostazione predefinita, il fattore di spam al livello **Consigliato** è del 59%. Questo significa che qualsiasi messaggio con una probabilità superiore al 59% sarà considerato *spam*.

Esistono in tutto cinque livelli di sensibilità (vedi 13.1 a pag. 196), tre dei quali (**Elevato, Raccomandato** e **Basso**) si basano su diversi valori del fattore di spam e probabile spam.

È possibile modificare autonomamente l'algoritmo Anti-Spam procedendo come segue:

1. Selezionare **Anti-Spam** nella sezione **Protezione**.
2. Nella sezione **Livello di protezione** sul lato destro della finestra fare clic su **Personalizza** e aprire la casella **Riconoscimento Spam** nella finestra di dialogo aperta (vedi Figura 62).
3. Nella finestra che si apre, regolare i fattori di spam e probabile spam nelle sezioni corrispondenti.

13.3.4. Creazione manuale di elenchi di mittenti e frasi Consentiti e Bloccati

L'utente può creare manualmente elenchi di mittenti e frasi Consentiti e Bloccati utilizzando Anti-Spam con i propri messaggi di posta elettronica. Questi elenchi contengono informazioni sugli indirizzi che l'utente considera sicuri o spam, e su varie parole chiave e frasi che identificano i messaggi come spam o non spam.

L'applicazione principale degli elenchi di espressioni chiave, in particolare l'Elenco Consentiti bianca, è la possibilità di coordinare con i destinatari attendibili, per esempio i colleghi, firme contenenti una determinata frase. Può trattarsi di una frase qualsiasi. Per esempio è possibile utilizzare come firma una firma PGP. È possibile utilizzare caratteri jolly nelle firme e negli indirizzi: ***** e **?**. L'asterisco * rappresenta una sequenza qualsiasi di caratteri di lunghezza non definita. Il punto interrogativo rappresenta un carattere singolo qualsiasi.

Se la firma contiene asterischi e punti interrogativi, per evitare errori durante l'elaborazione da parte di Anti-Spam essi devono essere preceduti da una barra rovesciata. Così al posto di un solo carattere ne vengono utilizzati due: ***** e **?**.

13.3.4.1. Indirizzi e frasi appartenenti all'Elenco consentiti

L'elenco consentiti contiene frasi ricorrenti individuate nei messaggi catalogati come *non spam*, e gli indirizzi dei mittenti dai quali si è certi che non potrebbe mai provenire un messaggio di spam. L'elenco delle frasi consentite viene compilata manualmente, mentre l'elenco degli indirizzi dei mittenti viene creato automaticamente durante l'apprendimento del componente Anti-Spam. L'elenco può essere modificato dall'utente.

Per configurare l'Elenco Consentiti:

1. Selezionare **Anti-Spam** nella sezione **Protezione**.
2. Fare clic sul pulsante **Personalizza** nella sezione **Livello di protezione** ed aprire la casella **Elenco Consentiti** (vedi Figura 63).

La tabella è suddivisa in due sezioni: quella superiore, contenente gli indirizzi dei mittenti di messaggi accettabili, e quella inferiore, contenente le frasi ricorrenti nei loro messaggi.

Per abilitare l'elenco consentiti di frasi e indirizzi durante il filtro dello spam, selezionare le caselle corrispondenti nelle sezioni **Mittenti consentiti** e **Frasi consentite**.

È possibile modificare gli elenchi servendosi degli appositi pulsanti in ciascuna sezione.

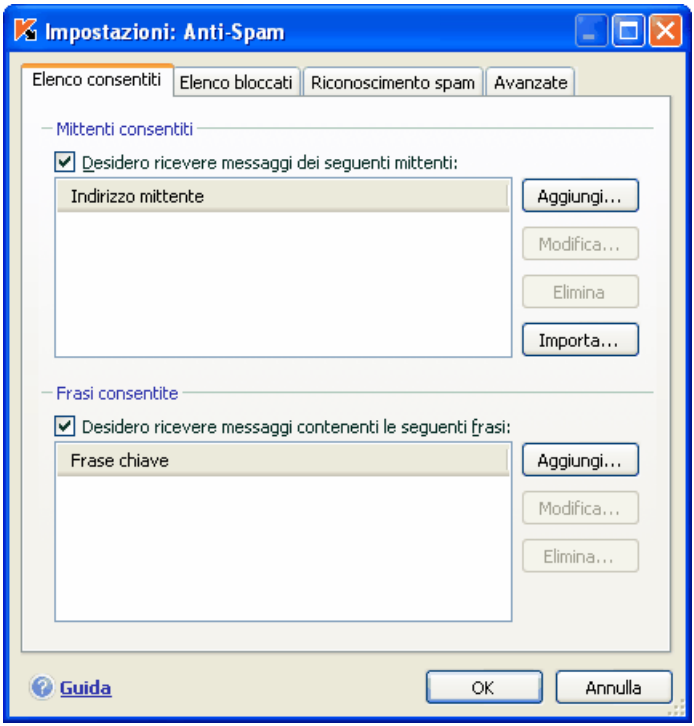


Figura 63. Configurazione dell'Elenco Consentiti di indirizzi e frasi

È possibile assegnare all'elenco dei mittenti sia indirizzi completi sia maschere di indirizzi. Durante l'inserimento di un indirizzo, le lettere maiuscole non vengono tenute in considerazione. Osserviamo alcuni esempi di maschere di indirizzi:

- *ivanov@test.ru* – i messaggi provenienti da questo indirizzo saranno sempre classificati come accettabili;
- **@test.ru* – i messaggi provenienti da qualsiasi indirizzo del dominio test.ru sono considerati accettabili, per esempio: *petrov@test.ru, sidorov@test.ru;*
- *ivanov@** – un mittente con questo nome, indipendentemente dal dominio di posta, è considerato sempre accettabile, per esempio: *ivanov@test.ru, ivanov@mail.ru*;
- **@test** – i messaggi provenienti da qualsiasi mittente di un dominio che inizia per test non vengono considerati spam, per esempio: *ivanov@test.ru, petrov@test.com*;

- *ivan.*@test.???* – i messaggi provenienti da un mittente il cui nome inizia con ivan. e il cui dominio inizia con test e finisce con qualsiasi sequenza di tre caratteri viene sempre considerato accettabile, per esempio: *ivan.ivanov@test.com, ivan.petrov@test.org*.

È possibile utilizzare maschere anche per le frasi. Durante l'inserimento di una frase, le lettere maiuscole non vengono tenute in considerazione. Ecco alcuni esempi:

- *Caro Ivan!* -- un messaggio contenente solo questo testo è considerato *accettabile*. Si sconsiglia di utilizzare questa frase per un elenco consentiti.
- *Caro, Ivan!** -- un messaggio che inizia con *Caro Ivan!* È considerato accettabile.
- *Caro *! * – i messaggi che iniziano con *Caro* e un punto esclamativo in qualsiasi punto del messaggio non sono considerati spam.
- *Ivan? * – il messaggio si rivolge a un utente di nome *Ivan*, il cui nome è seguito da qualsiasi carattere, e non è considerato spam.
- *Ivan\? * – i messaggi contenenti il gruppo *Ivan?* sono considerati accettabili.

Per disabilitare l'uso di un determinato mittente o frase come attributo di messaggio valido, non è necessario eliminarli dall'elenco, ma è sufficiente deselezionare le caselle accanto al testo corrispondente.

I mittenti dell'Elenco Consentiti possono essere importati dai file **.txt* o **.csv* o dalla rubrica di Microsoft Office Outlook/ Microsoft Outlook Express. Selezionando l'importazione da una rubrica, si apre un'altra finestra (vedi Figure 64). Sarà necessario selezionare quali oggetti di rubrica da quale client di posta devono essere importati nella rubrica di Anti-Spam.

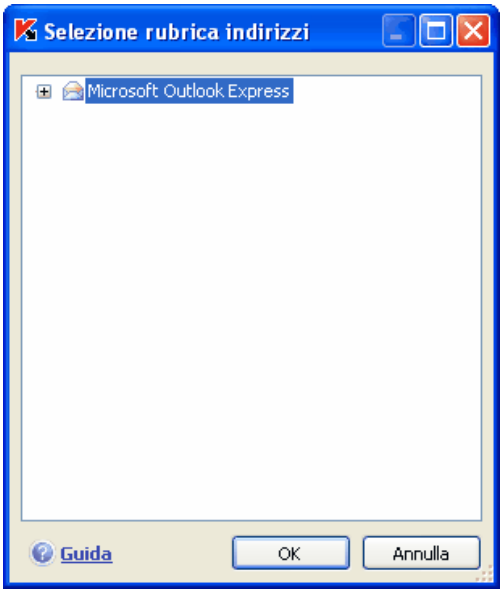


Figure 64. Selezione della rubrica

13.3.4.2. Indirizzi e frasi appartenenti all'Elenco bloccati

L'Elenco bloccati contiene frasi ricorrenti individuate nei messaggi classificati come *spam* nonché gli indirizzi di provenienza. L'elenco viene compilato manualmente.

Per compilare l'elenco bloccati:

1. Selezionare **Anti-Spam** nella sezione **Protezione**.
2. Fare clic sul pulsante **Personalizza** nella sezione **Livello di protezione** ed aprire la casella **Elenco bloccati** (vedi Figura 65).

La tabella è suddivisa in due sezioni: quella superiore, contenente gli indirizzi dei mittenti di messaggi spam, e quella inferiore, contenente le frasi ricorrenti nei loro messaggi.

Per abilitare l'Elenco bloccati di frasi e mittenti durante il filtro dello spam, selezionare le caselle corrispondenti nelle sezioni **Mittenti bloccati** e **Frasi bloccate**.

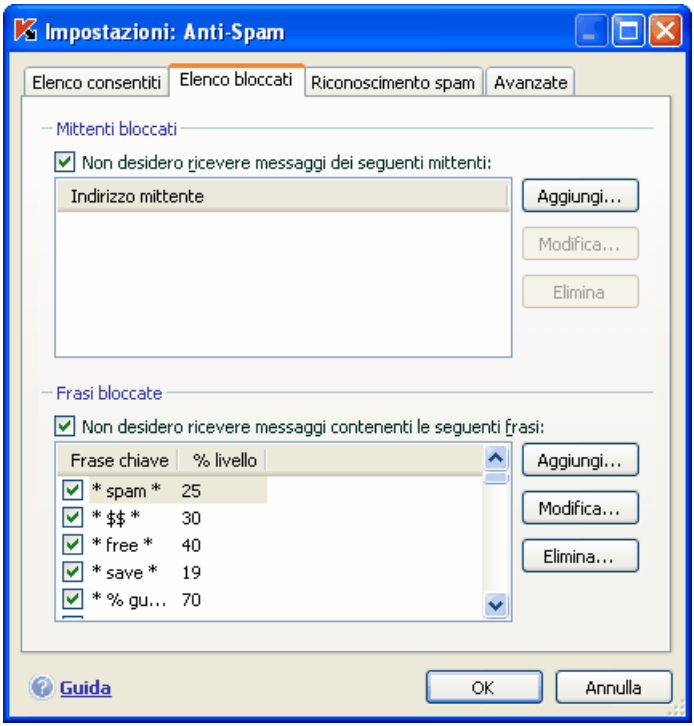


Figura 65. Configurazione dei mittenti e delle frasi appartenenti all'Elenco bloccati

È possibile modificare gli elenchi servendosi degli appositi pulsanti in ciascuna sezione.

È possibile assegnare alla lista dei mittenti sia indirizzi completi sia maschere di indirizzi. Durante l'inserimento di un indirizzo, le lettere maiuscole non vengono tenute in considerazione. Le maschere degli indirizzi possono essere utilizzate esattamente come per l'Elenco consentiti nella sezione precedente.

È possibile utilizzare maschere anche per le frasi. Durante l'inserimento di una frase, le lettere maiuscole non vengono tenute in considerazione. L'utilizzo delle frasi è identico a quanto decritto per le Liste Bianche.

Per disabilitare l'uso di un determinato mittente o frase come attributo di spam, tale mittente o frase può essere eliminato utilizzando il pulsante **Elimina**, o disabilitato deselezionando le caselle corrispondenti.

13.3.5. Funzioni avanzate di filtro antispam

Oltre alle principali funzioni utilizzate per il filtro dello spam (creazione di elenchi consentiti e bloccati, analisi antiphishing, tecnologie di filtro), è possibile avvalersi di funzioni avanzate.

Per configurare le funzioni avanzate di filtro antispam:

1. Selezionare **Anti-Spam** nella sezione **Protezione**.
2. Fare clic sul pulsante **Personalizza** nella sezione **Livello di protezione** ed aprire la scheda **Avanzate** (vedi Figura 66).

Essa contiene una serie di indicatori che classificano un messaggio e-mail come probabile spam.

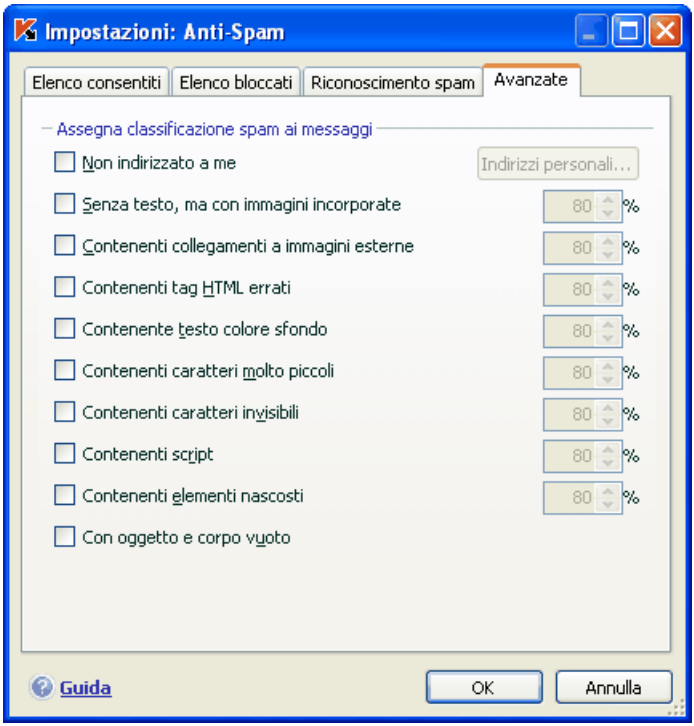


Figura 66. Impostazioni avanzate di riconoscimento dello spam

Per utilizzare eventuali indicatori supplementari di filtro, selezionare la casella corrispondente. Ciascuno degli indicatori richiede inoltre l'impostazione di un fattore di spam (in punti percentuali) che definisce la probabilità che un

messaggio sia classificato come spam. Il valore predefinito del fattore di spam è 80%. Il messaggio sarà classificato come spam se la somma delle probabilità di tutti i fattori supplementari supera il 100%.

Lo Spam può essere rappresentato da mail vuote (niente oggetto né testo), e-mail contenenti link a immagini o con immagini incluse, con testo dello stesso colore dello sfondo o con un font molto piccolo. Spam può essere anche una mail con testo con caratteri invisibili o con elementi nascosti, con tag html falsi oppure mail con script nocivi (istruzioni che il computer esegue quando l'utente apre la mail).

Se si abilita il filtro della posta "Non indirizzato a me", è necessario specificare l'elenco dei propri indirizzi nella finestra che si apre facendo clic su **Indirizzi personali**. L'indirizzo del destinatario verrà controllato durante la scansione, se non corrisponde a nessun indirizzo presente in rubrica, verrà classificato come *Spam*.

La rubrica personale può essere creata o modificata nella finestra **I**ndirizzi e-mail personali cliccando su **Aggiunti, Modifica** o **Elimina**.

13.3.6. Mail Dispatcher

Attenzione!

Mail Dispatcher è disponibile solo se si riceve posta per mezzo del protocollo POP3 e a condizione che il server POP3 supporta la visualizzazione delle intestazioni delle e-mail.

Mail Dispatcher è progettato per visualizzare l'elenco dei messaggi presenti sul server senza scaricarli sul computer. In tal modo è possibile rifiutare dei messaggi, risparmiando tempo e denaro e riducendo la probabilità di scaricare spam e virus sul computer.

Mail Dispatcher si apre se è stata selezionata la casella **Apri Recapito posta alla ricezione della posta** nelle impostazioni di Anti-Spam.

Per eliminare messaggi dal server senza scaricarli sul computer:

Selezionare le caselle sulla sinistra dei messaggi da eliminare e fare clic sul pulsante **Elimina**. I messaggi selezionati saranno eliminati dal server. Il resto della posta sarà scaricato sul computer dopo la chiusura della finestra di Mail Dispatcher.

Talvolta può essere difficile decidere se accettare un determinato messaggio solo sulla base del mittente e dell'oggetto. In certi casi Mail Dispatcher offre ulteriori informazioni scaricando anche le intestazioni dei messaggi.

Per visualizzare le intestazioni dei messaggi:

Selezionare il messaggio dall'elenco della posta in arrivo. Le intestazioni vengono visualizzate nella parte inferiore del modulo.

Esse non presentano dimensioni considerevoli, limitandosi il più delle volte a poche decine di byte, e non possono contenere codici nocivi.

Ecco un esempio in cui la visualizzazione delle intestazioni può essere utile: gli spammer hanno installato un programma nocivo sul computer di un collega che invia spam con il proprio nome utilizzando la rubrica del proprio client di posta. La probabilità di trovarsi nella rubrica del collega è estremamente elevata, rendendo quindi il computer bersaglio frequente di spam proveniente da lui. È impossibile stabilire a priori, sulla base del solo indirizzo del mittente, se il messaggio sia stato inviato dal collega o da uno spammer. È quindi utile consultare le intestazioni del messaggio per controllare attentamente chi ha inviato il messaggio, quando e quali sono le sue dimensioni, oltre a ricostruire il percorso compiuto dal messaggio tra il mittente e il server di posta del destinatario. Tutte queste informazioni dovrebbero essere presenti nell'intestazione del messaggio. In base ad esse è possibile decidere se sia veramente necessario scaricare quel messaggio dal server o se in effetti sia consigliabile eliminarlo.

Nota:

È possibile ordinare i messaggi in base a qualsiasi colonna dell'elenco. Per ordinarli fare clic sull'intestazione della colonna. Le righe vengono quindi riorganizzate in ordine crescente. Per modificare l'ordine di visualizzazione, fare di nuovo clic sull'intestazione della colonna.

13.3.7. Azioni da eseguire sui messaggi di spam

Se dopo la scansione si scopre che un messaggio è spam o probabile spam, le fasi successive della procedura di Anti-Spam dipendono dallo stato dell'oggetto e dall'azione selezionata. Per impostazione predefinita, i messaggi riconosciuti come *spam* o *probabile spam* vengono modificati: alla riga dell'oggetto vengono aggiunte le annotazioni **[!! SPAM]** o **[?? Probable spam]**.

È possibile selezionare ulteriori azioni da eseguire in caso di spam o probabile spam. In MS Outlook, Outlook Express e The Bat! esistono plug-in specifici per questo scopo. Per altri client di posta è possibile configurare delle regole di filtro.

13.3.8. Configurazione dell'elaborazione di spam in Microsoft Office Outlook

I messaggi classificati da Anti-Spam come *spam* o *probabile spam* vengono contrassegnati per impostazione predefinita da speciali annotazioni **[!! SPAM]** o **[?? Probable Spam]** nella riga dell'**Oggetto**.

In Outlook è possibile trovare ulteriori azioni per lo spam e il probabile spam nell'apposita scheda **Kaspersky Anti-Spam** nel menu **Strumenti→ Impostazioni** (vedi Figura 67).

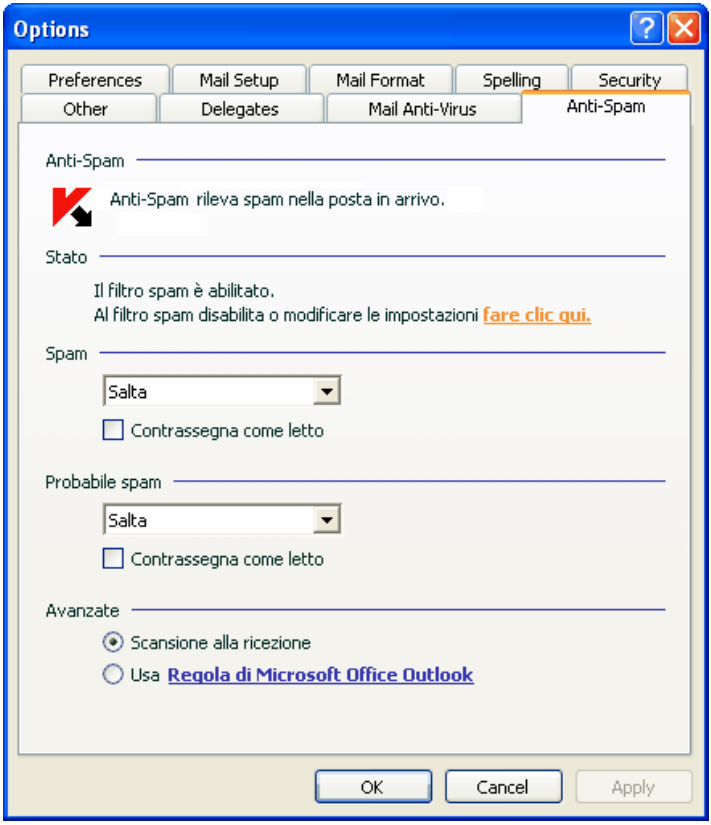


Figura 67. Configurazione dell'elaborazione di spam in Microsoft Office Outlook

Si apre automaticamente alla prima apertura del client di posta dopo l'installazione del programma e chiede se si desidera configurare l'elaborazione dello spam.

È possibile assegnare le seguenti regole sia ai messaggi di spam sia al probabile spam:

Sposta nella cartella – lo spam viene trasferito nella cartella specificata della casella di posta in arrivo.

Copia nella cartella – viene creata una copia del messaggio e trasferita nella cartella specificata. Il messaggio originale resta nella casella della posta in arrivo.

Elimina – elimina lo spam dalla casella della posta in arrivo dell'utente.

Salta – lascia il messaggio nella casella della posta in arrivo.

A tal fine, selezionare il valore appropriato dall'elenco a discesa della sezione **Spam** o **Probabile spam**.

È possibile inoltre configurare Microsoft Office Outlook e Anti-Spam in modo da lavorare congiuntamente:

- **Scansiona alla consegna**. Tutti i messaggi che entrano nella casella della posta in arrivo dell'utente vengono elaborati secondo le regole di Outlook. Al termine dell'elaborazione, il plug-in di Anti-Spam elabora i messaggi rimanenti che non rientrano in alcuna regola. In altre parole, i messaggi vengono elaborati secondo la priorità delle regole. Talvolta la sequenza delle priorità può essere ignorata se, per esempio, viene consegnato nella casella della posta in arrivo un gran numero di messaggi contemporaneamente. In tal caso possono verificarsi situazioni in cui le informazioni relative a un messaggio elaborato in base a una regola di Outlook vengono registrate nel report di Anti-Spam come *spam*. Per evitare questo inconveniente si raccomanda di configurare il plug-in di Anti-Spam come una regola di Outlook.
- **Usa regola di Microsoft Outlook**. Questa opzione consente di elaborare i messaggi in arrivo in base alla gerarchia delle regole di Outlook create. Una delle regole deve essere relativa all'elaborazione dei messaggi da parte di Anti-Spam. Si tratta della configurazione ottimale che non provoca conflitti tra Outlook e il plug-in di Anti-Spam. L'unico svantaggio di questa configurazione consiste nel fatto che occorre creare ed eliminare le regole di elaborazione dello spam manualmente attraverso Outlook.

Per creare una regola di elaborazione dello spam:

1. Aprire Microsoft Office Outlook e selezionare **Strumenti** → **Regole e Avvisi** nel menu principale. Il comando di apertura della creazione guidata dipende dalla versione di Microsoft Office Outlook. Questo manuale d'uso descrive come creare una regola utilizzando Microsoft Office Outlook 2003.

2. Nella finestra **Regole e Avvisi**, fare clic su **Nuova Regola** nella sezione **Regole e-mail**. La procedura guidata, accompagna l'utente attraverso le finestre e i passaggi che seguono:

   Passaggio 1

   È possibile scegliere di creare una regola *ex novo* o sulla base di un modello esistente. Selezionare **Crea nuova regola** e **Applica la regola dopo l'arrivo del messaggio**. Fare clic sul pulsante **Avanti**.

   Passaggio 2

   Nella finestra **Condizioni delle regole**, fare clic su **Avanti** senza selezionare alcuna casella. Confermare nella finestra di dialogo che si desidera applicare questa regola a tutti i messaggi ricevuti.

   Passaggio 3

   Nella finestra di selezione delle azioni da eseguire sui messaggi, selezionare la casella **Applica azione avanzata** dall'elenco delle azioni. Nella parte inferiore della finestra fare clic su azione avanzata. Nella finestra che si apre, selezionare **Kaspersky Anti-Spam** dal menu a discesa e fare clic su **OK**.

   Passaggio 4

   Nella finestra di selezione delle eccezioni alla regola, fare clic su **Avanti** senza selezionare alcuna casella.

   Passaggio 5

   Nella finestra finale della creazione guidata della regola è possibile modificarne il nome (il nome predefinito è **Kaspersky Anti-Spam**). Accertarsi che la casella **Applica regola** sia selezionata e fare clic su **Fine**.

3. Per impostazione predefinita alla nuova regola viene assegnata la prima posizione nell'elenco delle regole nella finestra **Regole messaggi**. Se lo si desidera, è possibile spostare questa regola in fondo all'elenco in modo da applicarla ai messaggi per ultima.

Tutti i messaggi in arrivo vengono elaborati in base a queste regole. L'ordine in cui il programma applica le regole dipende dalla priorità assegnata a ciascuna. Esse vengono applicate a partire dalla prima posizione dell'elenco. Ogni regola successiva occupa la posizione inferiore rispetto a quella che la precede. È possibile modificare la priorità di applicazione delle regole ai messaggi.

Se non si desidera continuare ad applicare ai messaggi una regola di Anti-Spam dopo averla usata una volta, occorre selezionare la casella **Interrompi l'elaborazione di ulteriori regole** tra le impostazioni delle regole (vedi il passaggio 3 della creazione di una regola).

Se si possiede una certa esperienza nella creazione di regole di elaborazione dei messaggi in Outlook, si possono creare regole personalizzate per Anti-Spam sulla base della configurazione suggerita.

13.3.9. Configurazione dell'elaborazione dello spam in Outlook Express (Windows Mail)

Attenzione!

Quando si abilita/disabilita il plugin di Microsoft Outlook Express, l'applicazione di posta elettronica deve essere riavviata.

Il plugin di Microsoft Outlook Express sarà disabilitato se si abilita la modalità di compatibilità di Kaspersky Internet Security con altre applicazioni (vedi 6.5 a pag. 77).

I messaggi classificati da Anti-Spam come *spam* o *probabile spam* vengono contrassegnati per impostazione predefinita da speciali annotazioni **[!! SPAM]** o **[?? Probabile Spam]** nella riga dell'**Oggetto**.

Ulteriori azioni da eseguire sui messaggi di spam e probabile spam in Outlook Express sono disponibili in una speciale finestra che si apre (vedi Figura 68) facendo clic sul pulsante **Impostazioni** accanto ai pulsanti di Anti-Spam sul pannello delle attività: **Spam** e **Non spam**.

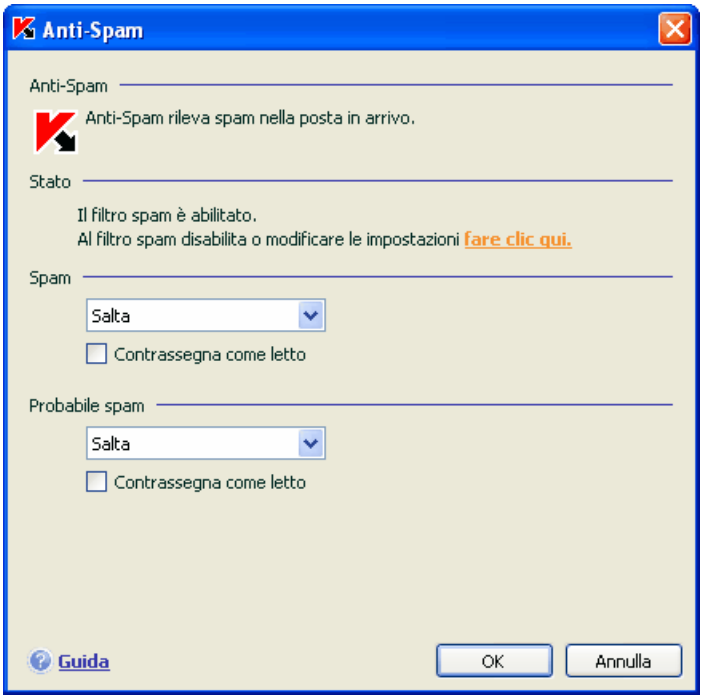


Figura 68. Configurazione dell'elaborazione dello spam in MS Outlook Express

Si apre automaticamente alla prima apertura del client di posta dopo l'installazione del programma e chiede se si desidera configurare l'elaborazione dello spam.

È possibile assegnare le seguenti regole sia ai messaggi di spam sia al probabile spam:

Sposta nella cartella – lo spam viene trasferito nella cartella specificata della casella di posta in arrivo.

Copia nella cartella – viene creata una copia del messaggio e trasferita nella cartella specificata. Il messaggio originale resta nella casella della posta in arrivo.

Elimina – elimina lo spam dalla casella della posta in arrivo dell'utente.

Ignora – lascia il messaggio nella casella della posta in arrivo.

A tal fine, selezionare il valore appropriato dall'elenco a discesa della sezione **Spam** o **Probabile spam**.

13.3.10. Configurazione dell'elaborazione dello spam in The Bat!

Le azioni per lo spam e il probabile spam in The Bat! sono definite mediante gli strumenti propri del client.

Per impostare le regole di protezione dello spam in The Bat!:

1. Selezionare **Impostazioni** dal menu **Opzioni** del programma di posta.
2. Selezionare **Anti-Spam** dalla struttura ad albero delle impostazioni (vedi Figura 69).

Le impostazioni di protezione antispam visualizzate valgono per tutti i moduli antispam installati nel computer che supportano The Bat!

È necessario impostare il livello di valutazione e specificare come reagire ai messaggio con un determinato punteggio (nel caso di Anti-Spam, la probabilità che il messaggio sia spam):

- Eliminare i messaggi con un punteggio più elevato di un determinato valore.
- Trasferire i messaggi con un determinato punteggio in una cartella specifica per lo spam.
- Trasferire nella cartella dello spam i messaggi contrassegnati da apposite intestazioni.
- Lasciare lo spam nella casella della posta in arrivo.

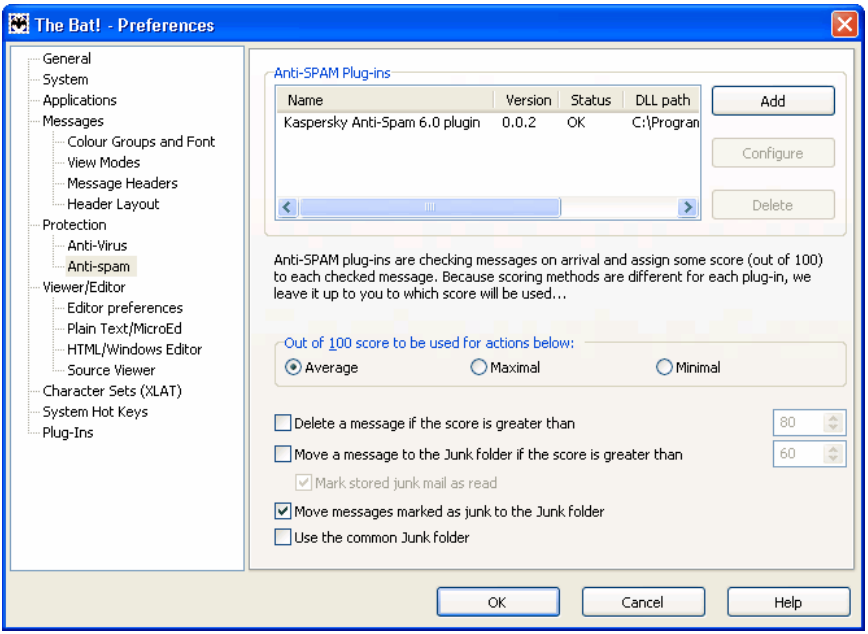


Figura 69. Configurazione del riconoscimento e dell'elaborazione dello spam in The Bat!

Attenzione!

Dopo aver elaborato un messaggio, Kaspersky Internet Security gli assegna uno stato di spam o probabile spam in base a un fattore (vedi 13.3.3 a pag. 177) con un valore regolabile dall'utente stesso. The Bat! possiede il proprio metodo di valutazione dello spam, basato anch'esso su un fattore di spam. Per garantire che non vi siano discrepanze tra il fattore di spam di Kaspersky Internet Security e quello di The Bat!, tutti i messaggi esaminati da Anti-Spam ottengono un punteggio conforme allo stato del messaggio: *Non spam* – 0%; *probabile spam* – *50 %*, spam – *100 %*.

In tal modo, il punteggio dello spam in The Bat! corrisponde non al fattore di spam assegnato in Anti-Spam ma al fattore dello stato corrispondente.

Per ulteriori informazioni sulle regole di valutazione e di elaborazione dello spam, consultare la documentazione relativa a The Bat!

CAPITOLO 14. CONTROLLO CONTENUTI

Controllo contenuti è un modulo di Kaspersky Internet Security che controlla l'accesso degli utenti a Internet. Il suo obiettivo è impedire l'accesso ai seguenti tipi di siti:

- Siti con contenuto per adulti o che contengono pornografia, armi, droghe, violenza, etc.
- Siti che possono portare a perdite di tempo (chat, giochi) o di denaro (e-commerce, gioco d'azzardo, ecc.).

E' importante sottolineare che spesso questi tipi di siti contengono spesso diversi programmi maligni; scaricare dati da siti di questo tipo può spesso portare ad un incremento del traffico Internet.

L'accesso degli utenti viene regolato dando ad ognuno un profilo per l'accesso ad Internet.

Un profilo consiste in un set di regole che controllano l'acceso dell'utente a qualunque sito. La decisione di bloccare o consentire l'accesso ad un sito viene presa comparando il suo indirizzo con i mittenti dell'Elenco consentiti e dell'Elenco bloccati a e classificando il contenuto di alcuni siti in categorie che devono essere bloccate.

Se non viene assegnato nessun profilo, di default è impostato il profilo **Bambino.** Un singolo profilo può essere assegnato anche a più account. Effettuando l'accesso tramite un profilo, l'utente può accedere solo ai siti consentiti dalle impostazioni del profilo stesso.

I profili **Adulto** e **Adolescente** possono essere protetti da password (vedi 14.2.1, p. 217). E' possibile attivare uno di questi profili solo inserendo la relativa password.

Ecco come funziona Controllo contenuti:

1. L'utente accede al sistema.
    - Se all'account con il quale l'utente accede al sistema non è stato assegnato nessuno dei profili disponibili, sarà caricato come impostazione predefinita il profilo più restrittivo rispetto agli altri, cioè **Bambino**;
    - Se il profilo assegnato a un account è disabilitato, a quell'account viene assegnato il profilo **Bambino**;

- Se l'account dell'utente è collegato a un dato profilo, viene caricato quel profilo.

2. L'utente accede ad un sito internet usando un computer con l'account controllato dal profilo attivo.

   Viene effettuata una verifica delle impostazioni di accesso (vedi 14.2.6, p. 224). L'URL della pagina richiesta viene controllato e comparato con gli indirizzi presenti nell'Elenco consentiti e nell'Elenco bloccati (vedi 14.2.3, p. 221) e il contenuto della pagina viene analizzato per capire se si tratta di un sito incluso nelle categorie proibite.

   Nel caso le azioni sopra descritte non rilevassero nulla di sospetto, l'indirizzo viene incluso nell'Elenco consentiti e la pagina internet viene caricata nel browser. Se una delle condizioni sopra descritte non viene rispettata, il sito viene bloccato.

3. All'utente non viene dato l'accesso ad un sito al quale cerca di accedere a causa di restrizioni sul profilo attivo. Per esempio, il profilo predefinito o il profilo di un altro utente con forti restrizioni è ancora attivo. Se l'utente ha accesso ad un altro profilo protetto da password, può inserire la password ed accedere a quel profilo. (vedi 14.1 pag. 216).

14.1. Passaggio a un altro profilo

Il profilo attivo può essere cambiato. Ciò può essere necessario se il profilo attivo ha restrizioni per l'accesso ad Internet.

Se si è a conoscenza delle password dei profili **Adulto** o **Adolescente** (non è possibile impostare password per il profilo **Bambino**), è possibile cambiare utente dalla finestra principale. Selezionare **Controllo contenuti** nella sezione **Protezione** e selezionare Usa Profilo. Selezionare il profilo desiderato ed inserire la password.

14.2. Impostazioni di Controllo contenuti

Attenzione!

Mentre si utilizza Controllo contenuti, si consiglia di impostare sempre delle password di protezione (vedi 19.9.2 pag. 305). Questo impedisce modifiche non autorizzate ai profili da parte di altri utenti.

Per configurare Controllo contenuti, seguire i seguenti passaggi:

- Assegnare i profili agli account utente (vedi 14.2.1, p. 217).
- Impostare una password per accedere al profilo selezionato (vedi 14.2.2 pag. 219).
- Impostare il livello di limitazione (vedi 14.2.2, p. 219) per ogni profilo e selezionare le impostazioni di filtro per il livello selezionato (vedi 14.2.3 pag. 221).
- Selezionare le azioni da intraprendere nel caso di accesso ad un sito non consentito (vedi 14.2.5, pag. 223).
- Impostare il tempo massimo di accesso a Internet per ogni profilo (vedi 14.2.6 pag. 224).

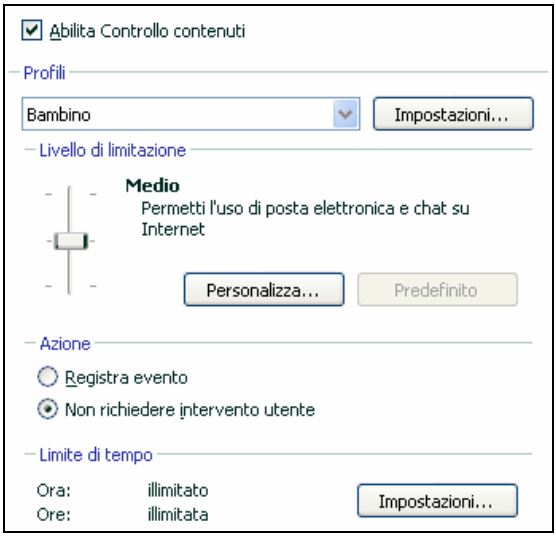


Figura 70. Configurazione di Controllo contenuti

14.2.1. Lavorare con i profili

Un *Profilo* è un set di regole che controllano l'accesso dell'utente a determinati siti web. I profili preinstallati sono tre:

- **Bambino** (profilo predefinito)
- **Adolescente**
- **Adulto**

Per ognuno di questi profili preinstallati, è già previsto un set di regole ottimale. Il profilo **Bambino** ha le restrizioni maggiori, mentre il profilo **Adulto** non ha restrizioni. I profili preinstallati non possono essere eliminati, ma i profili **Bambino** e **Adolescente** possono essere modificati a discrezione dell'utente.

Dopo l'installazione, **Bambino** è il profilo predefinito per tutti gli utenti a cui non è stato esplicitamente assegnato un profilo.

Per utilizzare i profili **Adolescente** e **Adulto**, selezionare la casella **Usa Profilo** nella finestra **Impostazioni: Profili** (vedi Figura 71). In questo modo, il profilo selezionato verrà mostrato nella lista **Profili** nella finestra di configurazione di **Controllo contenuti** (vedi Figura 70).

Nella sezione **Password** è possibile specificare una password per il profilo selezionato. Cambiare profilo ed accedere con il profilo al quale è stata impostata una password, non è possibile senza digitare la password stessa (vedi 14.1, p. 216). Se il campo **Password** viene lasciato vuoto, ogni utente potrà accedere tramite questo profilo. Il profilo **Bambino** non è protetto da password.

Nella sezione **Utenti** è possibile aggiungere utenti di Microsoft Windows cliccando su **Aggiungi** e selezionando l'account desiderato nella finestra di dialogo di Windows (vedi la guida del sistema operativo per maggiori dettagli).

Per eliminare un account da un profilo, selezionare l'account dalla lista e fare clic su **Elimina**.

Affinché Controllo contenuti funzioni in modo ottimale, si consiglia di collegare il profilo a un particolare account utente. Se si usano più profili su uno stesso account utente, si raccomanda di cancellare regolarmente la cache del proprio web browser (pagine web visitate, file temporanei, cookie, password salvate). In caso contrario, sussiste il rischio che le pagine web visitate da un utente con un profilo senza restrizioni siano visitate anche da un utente che ha invece le massime limitazioni.

Per modificare le impostazioni dei profili:

1. Aprire la finestra delle impostazioni e selezionare **Controllo contenuti** nella sezione **Protezione** (vedi Figura 70).
2. Selezionare il profilo preinstallato che si desidera modificare nella lista che si trova in **Profili** e fare clic su **Impostazioni.**

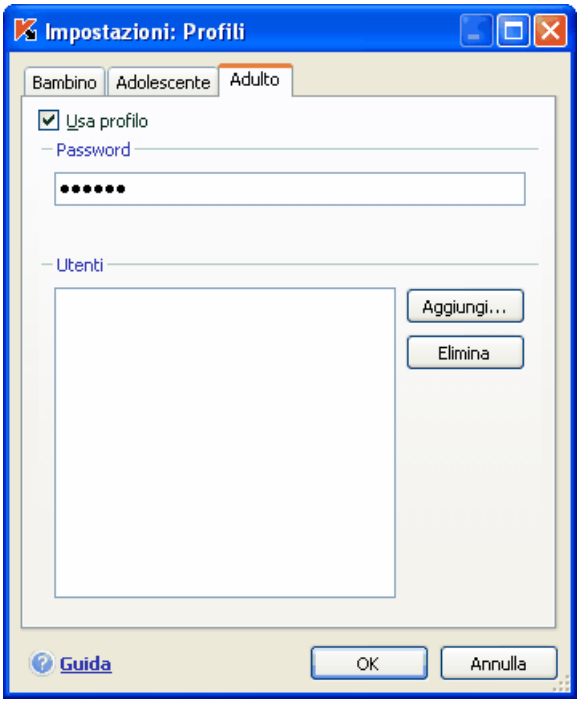


Figura 71. Profili di Controllo contenuti

14.2.2. Selezione del livello di limitazione

Controllo contenuti fornisce un controllo dell'accesso alle risorse Internet ad uno dei seguenti livelli (vedi Figura 72):

Alta: il livello al quale l'accesso ai siti di tutte le categorie è limitato (vedi 14.2.3 pag. 221).

Medio: queste impostazioni sono consigliate da Kaspersky Lab. Permette l'accesso a web mail e chat.

Alta: livello che permette l'accesso a tutta la rete ad esclusione delle categorie più "forti", come droghe, violenza, pornografia, ecc.

Il livello predefinito è impostato su **Medio.** Questo livello di accesso può essere aumentato o diminuito modificandone le impostazioni o riconfigurando il livello di sicurezza corrente.

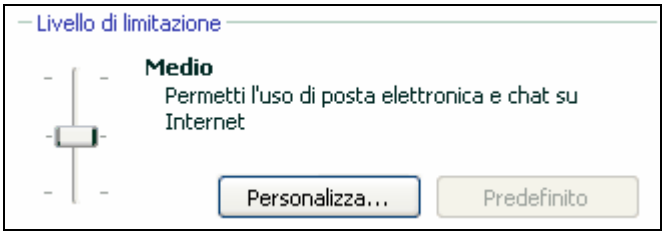


Figura 72. Selezione del livello di limitazione

Per modificare le impostazioni di un livello di limitazione:

Muovere il cursore. Modificando il livello, si definisce il numero di categorie di siti web bloccati che saranno presi in considerazione al momento della navigazione in Internet.

Se nessuno dei livelli soddisfa le esigenze dell'utente, è possibile personalizzarli. Selezionare il livello che maggiormente si avvicina alle proprie esigenze e modificarne le impostazioni. Questo modificherà il livello selezionato e diventerà personalizzato. Ecco un esempio di una situazione in cui ci sia bisogno di modificare un livello.

Esempio

Poniamo che si voglia impedire ai propri figli di visitare siti con contenuto per adulti o che possano causare perdite di tempo o denaro. Però, occorre anche inviare loro delle e-mail importanti.

Consiglio sulla scelta del livello

Selezionare il profilo **Bambino**. Il livello di limitazione **Alta** può essere usato come punto di partenza. Aggiungere il servizio di posta esterno con la casella di posta per il ragazzo all'Elenco consentiti; in questo modo il ragazzo potrà accedere solo alla posta.

Per cambiare il livello di limitazione corrente:

1. Aprire la finestra delle impostazioni e selezionare **Controllo contenuti** nella sezione **Protezione**.
2. Fare clic su **Personalizza** nella sezione **Livello di limitazione** (vedi Figura 72).
3. Modificare i paramenti di filtro nella finestra che si apre e cliccare su **OK**.

In questo modo si creerà un quarto livello di sicurezza con livelli di sicurezza personalizzati.

14.2.3. Impostazione del filtro

Le restrizioni all'acceso della rete vengono controllate da Controllo contenuti attraverso dei filtri. Un *Filtro* è un insieme di criteri utilizzati da Controllo contenuti per decidere si aprire o meno un particolare sito.

I siti possono essere filtrati in diversi modi:

- *Usando un Elenco consentiti*. In questo caso viene creato un elenco dei siti consentiti.
- *Usando un Elenco bloccati.* Questo metodo usa elenco di siti bloccati.
- *Usando Categorie bloccate.* In questo caso, il contenuto dei siti viene analizzato attraverso delle parole chiave per inserirli all'interno di categorie prestabilite. Se il numero di parole chiave all'interno di un sito supera la soglia stabilita, l'accesso viene bloccato.

Il database delle parole chiave e dei siti web è incluso in Kaspersky Internet Security e viene aggiornato contemporaneamente al programma.

> Nota:
>
> Le categorie bloccate elencate sono limitate a quelle predefinite. Non è possibile creare categorie bloccate personalizzate.

Per modificare le impostazioni di filtro del livello di limitazione selezionato:

1. Aprire la finestra delle impostazioni e selezionare **Controllo contenuti** nella sezione **Protezione**.
2. Fare clic su **Personalizza** nella sezione **Livello di limitazione** (vedi Figura 72).
3. Modificare i parametri del filtro in **Impostazioni Profilo: <nome profilo>** (vedi Figura 73).

Per configurare il filtro di un profilo, inserire i siti da bloccare e quelli autorizzati nei rispettivi elenchi (Consentiti e Bloccati).

Per modificare o eliminare gli indirizzi dagli elenchi, utilizzare gli appositi comandi.

Per creare un elenco dei siti bloccati o consentiti, è necessario inserire ogni indirizzo nel campo corrispondente nella finestra **Aggiunta di maschere degli indirizzi URL**.

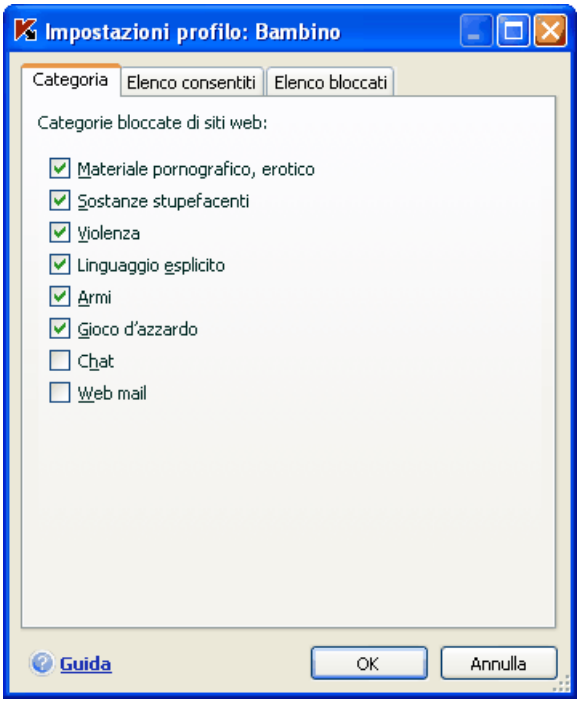


Figura 73. Configurazione delle impostazioni di filtro

Quando si inserisce un sito bloccato/consentito, è possibile creare delle maschere con i seguenti paramenti:

* - qualsiasi combinazione di caratteri

Esempio: Se si crea la maschera *abc*, nessun indirizzo che contiene abc sarà analizzato. Per esempio: www.virus.com/download_virus/page_0-9abcdef.html.

? - qualsiasi carattere.

Esempio: se si crea la maschera **Patch_123?.com**, gli indirizzi che contengono quella serie di caratteri e qualsiasi carattere dopo il 3, non verranno analizzati. Per esempio: **Patch_1234.com**. Invece **Patch_12345.com** verrà analizzato.

Se * o **?** sono realmente parte di un indirizzo aggiunto all'elenco, è necessario usare una barra rovesciata (\) per escludere l'***** o **?**, o **** dopo lo stesso.

Esempio: Si vuole aggiungere questo URL all'elenco dei siti consentiti:

www.virus.com/download_virus/virus.dll?virus_name=

Affinché Kaspersky Internet Security non elabori **?** come un carattere jolly, porre una barra rovesciata davanti al punto interrogativo. A questo punto, l'URL che si sta per aggiungere all'elenco delle esclusioni sarà come segue: www.virus.com/download_virus/virus.dll?virus_name=

14.2.4. Ripristino delle impostazioni predefinite del profilo

Quando si configura Controllo contenuti, c'è sempre la possibilità di utilizzare le impostazioni predefinite Queste sono considerate come ottimali e sono consigliate dagli specialisti Kaspersky; si trovano nel livello di sicurezza **Medio.**

Per ripristinare le impostazioni predefinite:

1. Aprire la finestra delle impostazioni e selezionare **Controllo contenuti** nella sezione **Protezione**.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di limitazione** (vedi Figura 72).

14.2.5. Configurazione delle azioni da intraprendere per tentativi di accesso non autorizzati

Se un utente cerca di accedere a un sito non consentito, il modulo Controllo contenuti eseguirà l'azione prevista nella sezione **Azione** (vedi Figura 71) nella finestra Controllo contenuti.

Per impostazione predefinita, Controllo contenuti blocca gli accessi e ne registra l'attività. Ecco un riassunto delle opzioni relative alle azioni intraprese in caso di tentativi di accesso non autorizzato.

Se si sceglie	Se è rilevato l'accesso non autorizzato a una risorsa di rete bloccata, il programma si comporta nel seguente modo
Registra evento	Il programma registrerà ogni tentativo di accesso a una risorsa web non consentita.
Non richiedere intervento utente	Il programma bloccherà l'accesso alla risorsa web non consentita e registrerà l'evento.

14.2.6. Accesso per un intervallo di tempo limitato

Il tempo di accesso ad Internet può essere configurato nella sezione **Limite di tempo** (vedi Figura 71) nella finestra delle impostazioni di Controllo contenuti. Fare clic su **Impostazioni** per configurare le restrizioni.

Selezionando l'opzione **Imposta limite tempo quot. di navigaz. In Internet**, è possibile specificare il tempo complessivo (in ore) di accesso a Internet nell'arco delle 24 ore.

Per limitare l'accesso ad Internet in orari particolare, spuntare la voce **Consente l'accesso a Internet ad ore specifiche** e impostare l'intervallo di tempo desiderato. A tal fine, cliccare su **Aggiungi** e nella finestra che si apre specificare l'orario. Per modificare l'intervallo utilizzare i comandi appositi.

Se vengono specificati due intervalli di tempo, di cui uno maggiore dell'altro, verrà preso in considerazione l'intervallo più piccolo.

Esempio: per il profilo **Bambino** si è inserito 3 ore come tempo massimo di accesso a Internet nell'arco di 24 ore e dalle 14.00 alle 15.00 come fascia oraria consentita. In questo modo, l'accesso a Internet sarà consentito solo dalle 14:00 alle 15:00, benché il numero di ore complessivo consentito fosse maggiore.

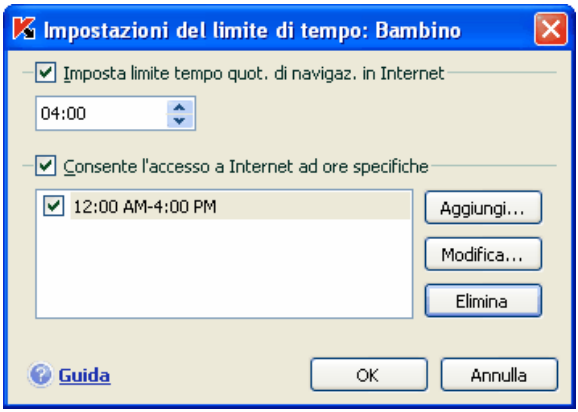


Figura 74. Accesso per un intervallo di tempo limitato

CAPITOLO 15. SCANSIONE ANTIVIRUS DEL COMPUTER

Un aspetto importante nella protezione di un computer dai virus è rappresentato dalla scansione anti-virus di aree definite dall'utente. Kaspersky Internet Security può operare tale scansione su singoli oggetti (file, cartelle, dischi, dispositivi rimovibili), o sull'intero computer. La scansione anti-virus impedisce la diffusione di quei codici dannosi che non sono stati individuati dai componenti di protezione in tempo reale.

Kaspersky Internet Security comprende le seguenti modalità di scansione predefinite:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer, ovvero: la memoria del sistema, i programmi caricati all'avvio, i settori di boot del disco fisso e le directory di sistema *Windows* e *system32*. Tale funzione ha lo scopo di individuare rapidamente i virus presenti nel sistema senza operare la scansione completa dello stesso.

Risorse del computer

Esegue la scansione del computer, con una ispezione completa di tutte le unità disco, della memoria e dei file.

Oggetti di avvio

Esegue la scansione anti-virus dei programmi caricati all'avvio del sistema operativo.

Scansione Rootkit

Esegue la scansione alla ricerca di rootkit che nascondono programmi maligni nel sistema operativo. Queste applicazioni si installano all'insaputa dell'utente, nascondono la loro presenza e nascondono qualunque attività che un programma maligno può effettuare su siti, cartelle, processi o chiavi di registro.

Le impostazioni raccomandate per queste modalità sono quelle predefinite. È possibile visualizzare tali impostazioni (vedi 15.4 pag. 231) o stabilire un programma (vedi 15.3 pag. 230) per l'esecuzione delle scansioni secondo dette modalità.

È inoltre possibile creare modalità di scansione personalizzate (vedi 15.3 a pagina 230) e pianificarne l'esecuzione. Ad esempio, è possibile pianificare la

scansione anti-virus dell'archivio della posta elettronica una volta la settimana, o la scansione della sola cartella **Documenti**.

È comunque possibile eseguire la scansione anti-virus di singoli oggetti (come ad esempio il disco fisso contenente programmi e giochi, l'archivio di posta elettronica prelevato al lavoro, un archivio allegato ad una e-mail, ecc.) senza dover impostare una modalità di scansione specifica. È sufficiente selezionare l'oggetto sul quale eseguire la scansione dall'interfaccia di Kaspersky Internet Security, o tramite i normali strumenti del sistema operativo Windows (ad esempio tramite **Explorer**, o direttamente dal **Desktop**, ecc.).

È possibile vedere la lista completa delle modalità di scansione del computer in **Scansione**.

E' possibile inoltre creare un disco di emergenza (vedi 19.4, p. 287) per ripristinare un sistema dopo l'attacco di un virus. A tal fine, fare clic su Crea disco di emergenza.

15.1. Gestione delle attività di scansione antivirus

La scansione antivirus può essere avviata manualmente, oppure in maniera automatica, a scadenze predefinite (vedi 6.7 pag. 79).

Per avviare manualmente un'attività di scansione:

Selezionare il nome dell'attività nella sezione **Scansiona** della finestra principale del programma, e fare clic su Avvia scansione.

Le azioni intraprese vengono mostrate in un menu apposito che appare cliccando con il tasto destro sull'icona dell'applicazione nell'area di notifica della barra applicazioni.

Per mettere in pausa un'attività:

Selezionare **Scansione** e nella finestra che appare cliccare Sospendi. In tal modo la scansione risulterà sospesa, e rimarrà tale fino a che non sarà riavviata manualmente, o fino all'occorrenza della successiva scansione programmata. Per avviare manualmente la scansione, fare clic su Ripristina.

Per terminare una scansione:

Selezionare **Scansione** e nella finestra che appare cliccare Interrompi. Ciò determinerà l'arresto della scansione, che potrà essere riavviata manualmente, o che sarà riavviata automaticamente alla successiva scansione programmata. Al successivo avvio di una scansione, il programma chiederà all'utente se desidera riprendere la scansione dal

punto in cui era stata precedentemente interrotta, o ricominciarla dal principio.

15.2. Creazione di un elenco di oggetti su cui eseguire una scansione

Per visualizzare un elenco di oggetti su cui operare una scansione secondo una determinata modalità, selezionare il tipo di scansione (ad esempio, **Computer**) nella sezione **Scansione** della finestra del programma principale. L'elenco degli oggetti sarà visualizzato sul lato destro della finestra, sotto la barra di stato (vedi Figura 76).

Figura 75. Elenco di oggetti su cui operare la scansione

Quando il programma viene installato, vengono già creati degli elenchi di oggetti su cui operare la scansione. Creando modalità di scansione personalizzate o selezionando un oggetto per la scansione, è possibile impostare un elenco di oggetti.

È possibile ampliare o modificare un elenco di oggetti utilizzando i pulsanti sulla destra dell'elenco. Per aggiungere un oggetto all'elenco, cliccare sul pulsante **Aggiungi**; si aprirà una finestra nella quale selezionare l'oggetto su cui eseguire la scansione.

Per comodità, è possibile aggiungere delle categorie di aree da sottoporre a scansione come ad esempio database di e-mail, oggetti in esecuzione all'avvio, backup del sistema operativo, ecc.

Inoltre, quando si aggiunge una cartella che contiene sottocartelle è possibile aggiungerle all'area da scansionare. A tal fine, selezionare la cartella e nel menu contestuale selezionare l'opzione **Includi sottocartelle.**

Per eliminare un oggetto, selezionarlo nell'elenco (così facendo, il nome dell'oggetto verrà evidenziato in grigio) e cliccare sul pulsante **Elimina**. È possibile disabilitare temporaneamente la scansione su determinati oggetti di un elenco, senza doverli eliminare. A tal fine, è sufficiente deselezionare gli oggetti in questione, che saranno ignorati dalla scansione.

Per avviare una scansione, cliccare su Avvia scansione.

Oltre a questo, è possibile selezionare un oggetto su cui eseguire una scansione anche utilizzando gli strumenti del sistema operativo Windows (ad esempio tramite la finestra di **Explorer**, o direttamente dal Desktop, ecc.) (vedi Figura 76). A tal fine, posizionare il cursore sul nome dell'oggetto in questione, aprire il menu contestuale di Windows facendo clic con il pulsante destro del mouse, e selezionare **Avvia**.

Figura 76. Scansione di oggetti attraverso il menu contestuale di Windows

15.3. Creazione di attività di scansione antivirus

Per eseguire la scansione antivirus di oggetti presenti sul computer, è possibile utilizzare le modalità di scansione predefinite offerte dal programma o crearne di nuove. Queste ultime vengono create a partire da attività di scansione preesistenti.

Per creare una nuova attività di scansione antivirus:

1. Selezionare, nella sezione **Scansione** della finestra del programma principale, la modalità di scansione le cui impostazioni si avvicinano maggiormente a quelle desiderate.
2. Aprire il menu contestuale facendo clic con il pulsante destro del mouse e selezionare **Salva con nome** o fare clic su Nuova operazione di scansione.
3. Nella finestra che appare, inserire il nome della nuova modalità di scansione e premere **OK**. Nell'elenco delle modalità di scansione, nella sezione **Scansione** della finestra del programma principale, figurerà una nuova modalità col nome appena inserito.

Attenzione!

Un utente può creare un massimo di quattro modalità di scansione.

La nuova attività di scansione eredita tutte le proprietà di quella da cui è stata creata. Per mettere ulteriormente a punto la nuova attività è necessario creare l'elenco di oggetti su cui operare la scansione (vedi 15.2 a pag. 228), impostare le proprietà (vedi 15.4 a pag. 231) della modalità stessa, e, se necessario, configurare un programma (vedi 6.6 on pag. 78) per l'esecuzione automatica della scansione.

Per rinominare un'attività di scansione esistente:

Selezionare l'attività da rinominare nella sezione **Scansione** della finestra del programma principale, fare clic col pulsante destro del mouse per aprire il menu contestuale e selezionare Rinomina.

Per eliminare un'attività di scansione esistente:

Selezionare l'attività da eliminare nella sezione **Scansione** della finestra del programma principale, fare clic con il pulsante destro del mouse per aprire il selezionare e selezionare Elimina.

Apparirà una finestra nella quale verrà chiesto all'utente di confermare l'operazione di eliminazione. A conferma avvenuta, l'attività di scansione

eliminata non sarà più presente nell'elenco delle attività della sezione **Scansione**.

Attenzione!

È possibile rinominare o eliminare soltanto le modalità di scansione create dall'utente.

15.4. Configurazione delle attività di scansione antivirus

Il metodo impiegato per operare la scansione degli oggetti presenti nel computer dipende da un insieme di proprietà assegnate a ciascuna modalità.

Per configurare le impostazioni delle modalità di scansione:

Selezionare il nome dell'attività nella scheda **Scansione** della finestra principale e usare il link Impostazioni per aprire la finestra delle impostazioni.

Per ciascuna scansione, è possibile utilizzare tale finestra al fine di:

- Selezionare un livello di sicurezza per la modalità di scansione (vedi 15.4.1 pag. 232).
- Modificare le impostazioni avanzate:
  - Definire i tipi di file da sottoporre a scansione (vedi 15.4.1 a pag. 232).
  - Configurare l'avvio dell'attività utilizzando un profilo utente diverso (vedi 15.4.2 a pag. 233).
  - Configurare le impostazioni di scansione avanzate (vedi 15.4.3 a pag. 236).
  - Attivare la scansione dei rootkit (vedi 15.4.6 pag. 240) e l'analizzatore euristico (vedi 15.4.7a, p. 240).
- Ripristinare le impostazioni di scansione predefinite (vedi 15.4.6 pag 240).
- Selezionare l'azione che il programma deve intraprendere non appena venga rilevato un oggetto infetto, o presunto tale (vedi 15.4.7, p. 240).
- Creare un programma (vedi 6.7, p. 79) di avvio automatico delle scansioni.

È inoltre possibile configurare delle impostazioni globali (vedi 15.4.8, p. 242) applicabili a tutte le modalità di scansione.

Questa sezione del manuale d'uso esaminerà in dettaglio tutte le impostazioni sopra citate.

15.4.1. Selezione del livello di sicurezza

Ogni operazione di scansione anti-virus, in qualsiasi modalità, può eseguire l'analisi degli oggetti del computer ad uno di questi livelli (vedi Figura 77):

Protezione massima – massima accuratezza della scansione dell'intero computer, o di singoli dischi, cartelle o file. Se ne raccomanda l'impiego qualora si sospetti che un virus possa essere penetrato nel computer.

Consigliato. È il livello consigliato dagli esperti Kaspersky Lab. La scansione funziona in maniera analoga al livello **Protezione massima**, fatta eccezione per i database di posta elettronica.

Alta velocità – livello che permette all'utente un agevole impiego di applicazioni che utilizzino estensivamente le risorse della macchina, poiché la gamma dei file sottoposti a scansione è ridotta.

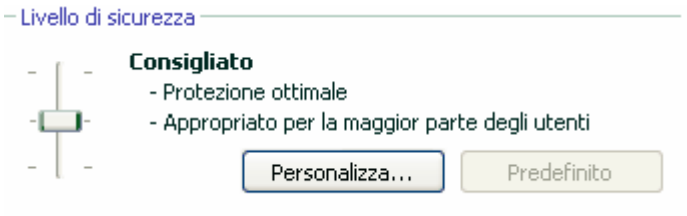


Figura 77. Selezione di un livello di sicurezza per la scansione antivirus

Per impostazione predefinita, il livello di sicurezza di File Anti-Virus è impostato su **Consigliato**.

È possibile aumentare o diminuire la sicurezza della scansione anti-virus selezionando il livello desiderato, oppure cambiando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Regolando il livello di sicurezza, si definisce il rapporto tra la velocità di scansione e il numero totale di file esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di file esaminati.

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzarne le impostazioni di protezione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer e utilizzarlo come

modello per modificare le impostazioni. In questo caso il livello diventa **personalizzato**.

Per modificare le impostazioni di un livello di sicurezza:

1. Aprire la finestra delle impostazioni e selezionare la voce **Scansione**.
2. Fare clic su **Personalizza** nella sezione **Livello di sicurezza** (vedi Figura 77).
3. Modificare i parametri nella finestra che appare e cliccare **OK**.

15.4.2. Definizione del tipo di oggetti da sottoporre a scansione

Quando si specificano i tipi di oggetti da analizzare, si stabilisce il formato dei file, la dimensione e le unità che saranno sottoposti a scansione anti virus in una specifica modalità.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (vedi Figura 78):

- **Esamina tutti i file**. Con questa opzione, tutti gli oggetti vengono sottoposti a scansione, senza eccezioni.
- **Esamina programmi e documenti (in base al contenuto)**. Selezionando questo gruppo di programmi, si sottopongono a scansione solo i file a rischio di infezione – quelli in cui si potrebbe nascondere un virus.

  Nota:

  Vi sono file nei quali non possono annidarsi virus, poiché il codice di tali file non contiene alcun elemento a cui il virus possa attaccarsi, Un esempio è costituito dai file .txt.

  Viceversa, ci sono alcuni tipi di file che possono contenere codice eseguibile. Alcuni esempi: exe, dll o doc. Il rischio di trovare e attivare codici maligni attraverso questi file è molto alto.

  Prima di cercare un virus in un oggetto, la sua intestazione interna viene analizzata per rilevarne il formato (txt, doc, exe, ecc.).

- **Esamina programmi e documenti (in base all'estensione)**. In questo caso, il programma sottoporrà a scansione solamente i file potenzialmente infetti, determinandone il formato in base all'estensione. Utilizzando il link, è possibile accedere ad un elenco di estensioni file che, con questa opzione, vengono sottoposti a scansione (vedi A.1 a pagina 334).

Suggerimento:

Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Esamina programmi e documenti (in base all'estensione)**, tale file sarebbe escluso dalla scansione. Invece, selezionando l'opzione **Esamina programmi e documenti (in base al contenuto)**, il programma ignorerà l'estensione del file analizzandone invece l'intestazione, e determinando così la sua vera natura di file eseguibile. Il file sarebbe quindi sottoposto a un'approfondita scansione antivirus.

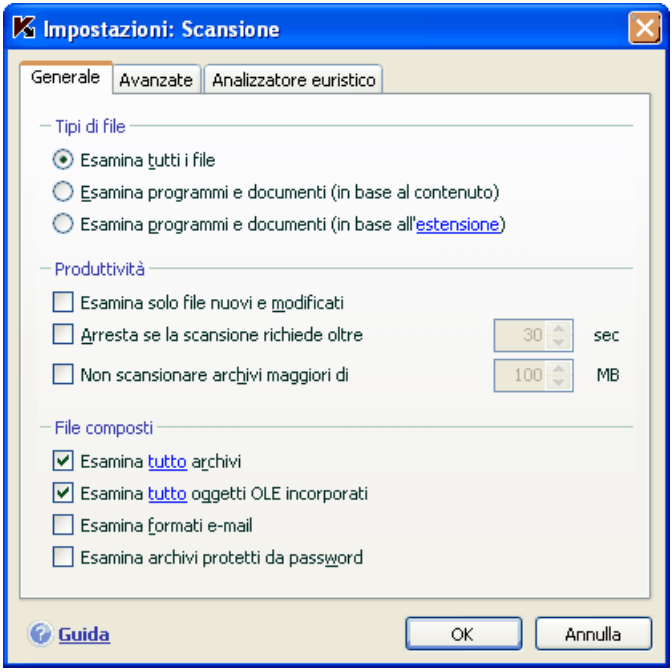


Figura 78. Configurazione delle impostazioni di scansione

Nella sezione **Produttività**, è possibile specificare se si vuole sottoporre a scansione solamente i nuovi file, oppure i nuovi file e quelli che sono stati modificati dopo la scansione precedente. Questa modalità riduce considerevolmente la durata della scansione e aumenta la velocità del programma. Per attivare questa modalità, selezionare la casella **Esamina solo file nuovi e modificati**. Questa modalità si applica sia ai file semplici sia a quelli composti.

Nella sezione **Produttività** si possono inoltre stabilire limiti di tempo e di dimensione dei file per la scansione.

- **Arresta se la scansione richiede oltre ... sec**. Selezionare questa opzione ed inserire la durata massima per la scansione di un singolo oggetto. Se la scansione di un oggetto richiede un tempo superiore a quello specificato, l'oggetto viene rimosso dalla coda di scansione.
- **Non scansionare archivi maggiori di … MB**. Selezionare questa opzione ed inserire la dimensione massima dell'oggetto. Se la dimensione di un oggetto supera quella specificata, l'oggetto viene rimosso dalla coda di scansione.

Nella sezione **File composti**, specificare quali file composti debbano essere sottoposti a scansione anti-virus:

- **Esamina Tutti/Solo nuovi archivi** – analizza gli archivi con estensione .rar, .arj, .zip, .cab, .lha, .jar, e .ice.

Attenzione!

Kaspersky Internet Security non elimina automaticamente formati di file compressi che non supporta (ad esempio .ha, .uue, .tar), anche se viene selezionata l'opzione di riparazione o eliminazione automatica dei file che non possono essere disinfettati.

Per eliminare questi tipi di file compressi, fare clic sul link Elimina Archivi nella notifica di rilevamento di oggetti pericolosi. Questa notifica sarà visualizzata sullo schermo dopo che il programma avrà iniziato a elaborare gli oggetti rilevati durante la scansione. Questi archivi possono anche essere eliminati manualmente.

- **Esamina Tutti/Solo nuovi oggetti OLE incorporati** – analizza gli oggetti incorporati nei file (per esempio fogli di calcolo di Excel o macro incorporati in un file di Microsoft Word, allegati di posta, ecc.).

Per ogni tipo di file composto è possibile selezionare ed esaminare tutti i file o solo quelli nuovi usando il link a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Produttività** è stata impostata in modo da esaminare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file complesso da sottoporre a scansione.

- **Esamina formati e-mail** – esegue la scansione dei file e dei database di posta elettronica. Se questa casella non è selezionata, il programma non opera la scansione di tali oggetti, e il loro stato, nel report, sarà indicato come *ok*.

In merito alla scansione di database di posta elettronica protetti da password, si prega di notare quanto segue:

Kaspersky Internet Security rileva i codici nocivi presenti nei database di Microsoft Office Outlook 2000, ma non li disinfetta;

Il programma non supporta la scansione dei codici nocivi dei database protetti di Microsoft Office Outlook 2003.

Esamina archivi protetti da password – esegue la scansione di archivi protetti da password. Se questa opzione è attiva, una finestra richiederà l'inserimento di una password prima che venga eseguita la scansione di un oggetto archiviato. Se la casella non è selezionata, la scansione ignorerà gli archivi protetti.

15.4.3. Impostazioni di scansione avanzate

In aggiunta alla configurazione base, è possibile anche utilizzare impostazioni avanzate (vedi Figura 79):

Usa tecnologia iChecker – tecnologia che permette di velocizzare la scansione escludendo alcune aree. Un oggetto viene escluso dalla scansione usando un algoritmo specifico che tiene conto della data di pubblicazione dei database dell'applicazione, della data dell'ultima scansione e delle modifiche alle impostazioni di scansione.

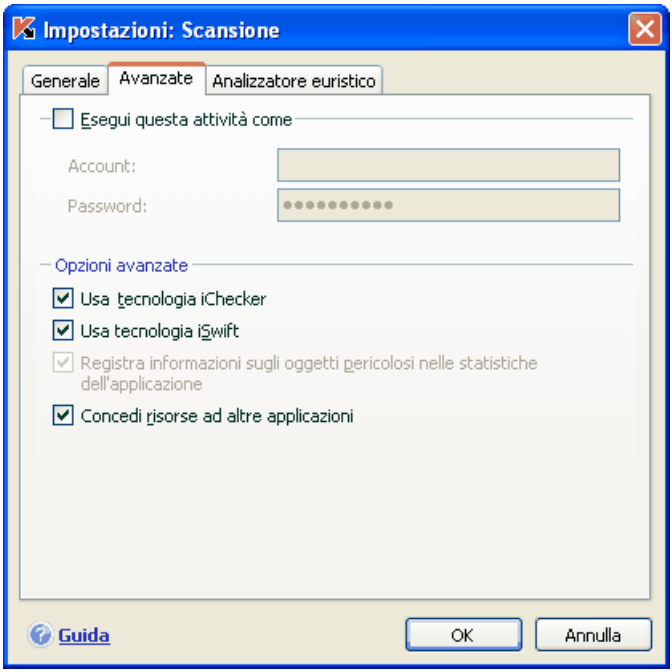


Figura 79. Impostazioni di scansione avanzate

Per esempio, se si è archiviato un file già sottoposto a scansione ed è stato considerato "non infetto", il programma non analizzerà questo archivio alla prossima scansione, sempre che non sia stato modificato o che le impostazioni di scansione non siano cambiate. Se la struttura dell'archivio è stata modificata perché un nuovo oggetto vi è stato aggiunto, o se il database del programma è stato aggiornato, l'antivirus effettuerà nuovamente la scansione.

iChecker presenta delle limitazioni: non funziona con i file di grandi dimensioni e si applica solo agli oggetti con una struttura che Kaspersky Internet Security riconosce (ad esempio *.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar*).

Usa tecnologia iSwift. Questa è un'evoluzione di iChecker pensata per i computer che utilizzano un file system NTFS. Anche iSwift presenta limitazioni: si limita a file system che si trovano in una specifica posizione e può essere applicata solo a oggetti in un file system NTFS.

Registra informazioni sugli oggetti pericolosi nelle statistiche dell'applicazione – salva informazioni sugli oggetti pericolosi rilevati nelle statistiche globali dell'applicazione e mostra un elenco delle minacce nella

scheda **Rilevato** della finestra dei report (vedi 19.3.2, p. 273). Se questa casella è deselezionata, i dati sugli oggetti pericolosi non saranno registrati nel report; pertanto tali oggetti non potranno essere elaborati.

Concedi risorse ad altre applicazioni – sospende l'attività di scansione antivirus se il processore è occupato da altre applicazioni.

15.4.4. Scansione dei rootkit

Un rootkit è rappresentato da un insieme di utility utilizzate per nascondere le tracce dei virus all'interno del sistema operativo. Queste utility si infiltrano nel sistema operativo, mascherano sia la loro presenza che quella di processi, cartelle e chiavi di registro che appartengono al virus descritto nella configurazione del rootkit.

La scansione dei rootkit può essere effettuata da un qualsiasi tipo di scansione (a condizione che questa opzione sia abilitata per quella specifica attività); ad ogni modo gli esperti di Kaspersky Lab hanno creato un'operazione di scansione apposita dedicata esclusivamente alla ricerca di rootkit.

Per abilitare la scansione dei rootkit, spuntare la casella **Abilita rilevamento rootkit** nella sezione **Scansione Rootkit.** Se la scansione è abilitata, un più accurato livello di scansione può essere impostato selezionando **Abilita scansione rootkit estesa.** In questo modo, la scansione cercherà in maniera più approfondita la presenza di eventuali rootkit, analizzando una più ampia gamma di oggetti. Queste voci sono deselezionate di default, dato che tale operazione richiede molte risorse di sistema.

Per configurare la scansione dei rootkit:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare la voce **Scansione**.
2. Fare clic su **Personalizza** nella sezione **Livello di sicurezza** (vedi Figura 77) e selezionare la scheda **Analizzatore Euristico** nella finestra che si è aperta (vedi Figura 80).

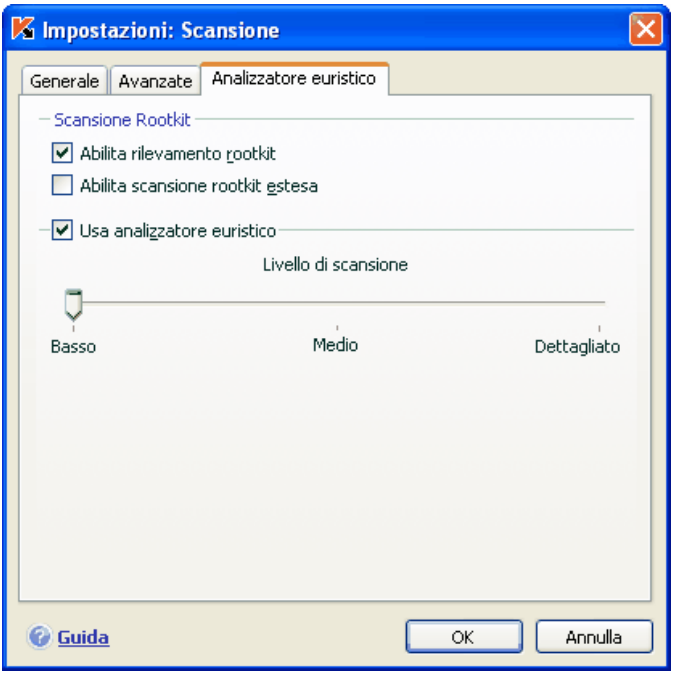


Figura 80. Configurazione della scansione dei rootkit e dei metodi euristici

15.4.5. Utilizzo dei metodi euristici

I metodi euristici sono utilizzati da alcuni componenti della protezione in tempo reali e attività di scansione anti-virus (vedi 7.2.4, p. 103 per maggiori dettagli).

La scheda **Analizzatore Euristico** (vedi Figura 80) può essere usata per abilitare /disabilitare l'analizzatore euristico per le minacce sconosciute. A tal fine, eseguire i seguenti passaggi:

1. Aprire la finestra delle impostazioni e selezionare un'attività sotto la voce **Scansione**.
2. Fare clic su **Personalizza** nella sezione **Livello di sicurezza** e aprire la scheda **Analizzatore Euristico** nella finestra di dialogo che si è aperta.

Per utilizzare il metodo euristico, selezionare **Usa Analizzatore Euristico.** Un ulteriore livello di precisione può essere impostato muovendo il cursore su un dei seguenti livelli:**Basso, Medio** o **Dettagliato**.

15.4.6. Ripristino delle impostazioni di scansione predefinite

Quando si configurano le impostazioni per una data modalità di scansione, è sempre possibile ripristinare le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Consigliato**.

Per ripristinare le impostazioni di scansione anti-virus predefinite:

1. Aprire la finestra delle impostazioni e selezionare un'attività sotto la voce **Scansione**.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza** (vedi Figura 77).

15.4.7. Selezione delle azioni da applicare agli oggetti

Se durante una scansione viene rilevato un file infetto, o presunto tale, il programma reagirà in base allo stato dell'oggetto e all'azione selezionata.

All'oggetto in questione può essere assegnato, dopo la scansione, uno dei seguenti stati:

- Programma nocivo (per esempio, *virus, trojan*).
- *Potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. È probabile che il programma abbia rilevato una sequenza di codice nel file tratta da un virus sconosciuto o da un codice modifica di un virus noto.

Per impostazione predefinita, tutti i file infetti sono sottoposti a un tentativo di riparazione e se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

Aprire la finestra delle impostazioni e selezionare la voce **Scansione**. Tutte le azioni possibili vengono visualizzate nella sezione apposita (vedi Figura 81).

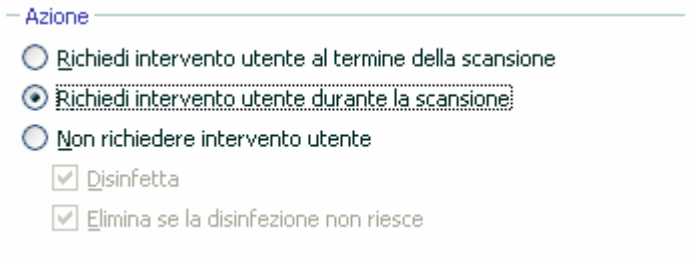


Figura 81. Selezione di un'azione per gli oggetti pericolosi

Se l'azione selezionata è	**Se viene rilevato un oggetto dannoso o potenzialmente infetto**
Richiedi intervento utente al termine della scansione	Il programma non interviene sugli oggetti prima della fine della scansione. Al termine del processo, una finestra di statistiche relative alla scansione appena ultimata mostrerà l'elenco degli oggetti rilevati, chiedendo all'utente se intervenire su di essi o meno.
Richiedi intervento utente durante la scansione	Il programma mostrerà un messaggio di allarme contenente informazioni sul codice dannoso che ha, o che potrebbe avere infettato un file, e offrirà all'utente la possibilità di scegliere tra una delle seguenti azioni.
Non richiedere intervento utente	Il programma registra nel rapporto le informazioni relative agli oggetti rilevati, senza intervenire su di essi e senza notificare la cosa all'utente. Si sconsiglia di avvalersi di questa opzione, poiché gli oggetti dannosi permangono sul computer, ed è praticamente impossibile evitare l'infezione.
Non richiedere intervento utente **Disinfetta**	Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Qualora l'oggetto non possa essere disinfettato, gli viene assegnato

	lo stato Potenzialmente infetto e il programma provvederà a porlo in quarantena (vedi 19.1 a pag. 263). Le informazioni relative all'evento vengono registrate nel report (vedi 19.3 a pag. 269). In un secondo momento sarà possibile tentare di disinfettare l'oggetto.
Non richiedere intervento utente **Disinfetta** **Elimina se la disinfezione non riesce**	Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la disinfezione non riesce, l'oggetto viene eliminato.
Non richiedere intervento utente **Disinfetta** **Elimina**	Il programma elimina automaticamente l'oggetto rilevato.

Quando disinfetta o elimina un oggetto, Kaspersky Internet Security ne crea una copia di backup e la invia a Backup (vedi 19.2 a pagina 267) cosicché l'oggetto rimanga disponibile qualora risulti necessari ripristinarlo, o emerga l'opportunità di disinfettarlo in un secondo momento.

15.4.8. Configurazione di impostazioni di scansione globali per tutte le attività

Ogni operazione di scansione viene eseguita secondo le relative impostazioni. Per impostazione predefinita, le attività di scansione create al momento dell'installazione del programma utilizzano le impostazioni raccomandate dagli esperti di Kaspersky Lab.

È possibile definire delle impostazioni globali valide per tutte le operazioni di scansione. Come termine di riferimento si utilizza un gruppo di proprietà applicabili alla scansione anti-virus di un singolo oggetto.

Per assegnare impostazioni di scansione globali:

1. Aprire la finestra delle impostazioni e selezionare la voce **Scansione**.
2. Configurare le impostazioni di scansione: Selezionare il livello di sicurezza (vedi 15.4.1 a pag. 206), configurare le impostazioni avanzate, e selezionare un'azione (vedi 15.4.7 a pag. 210) per gli oggetti.

3. Per rendere queste impostazioni valide per tutte le operazioni, cliccare sul pulsante **Applica** nella sezione **Altre impostazioni attività**. Confermare le impostazioni globali selezionate nella successiva finestra di dialogo.

CAPITOLO 16. TEST DELLE FUNZIONI DI KASPERSKY INTERNET SECURITY

Dopo aver installato e configurato Kaspersky Internet Security, si consiglia di controllare che le impostazioni del programma siano corrette utilizzando virus di prova e relative variazioni.

16.1. Il test EICAR e le sue varianti

eicar (European Institute for Computer Antivirus Research) ha sviluppato un programma simile ad un virus per testare le funzionalità dei programmi antivirus.

Il virus di prova NON E' UN VIRUS VERO E PROPRIO e non contiene un codice di programma che potrebbe danneggiare il computer in alcun modo. Però è stato creato in modo da essere riconosciuto dai programmi antivirus.

Mai utilizzare virus reali per testare le funzioni dell'antivirus!

E' possibile scaricare il virus per il test dal sito di EICAR: http://www.eicar.org/anti_virus_test_file.htm.

Il file scaricato dal sito EICAR contiene il corpo di un virus di prova standard. Per questo motivo Kaspersky Internet Security lo rileva, lo classifica come **virus** e agisce come da impostazione decisa dall'utente.

Per testare la reazione di Kaspersky Internet Security quando vengono rilevati diversi tipi di oggetti, è possibile modificare il contenuto del virus di prova standard aggiungendo uno dei prefissi indicati in tabella.

Prefisso	**Stato del virus di prova**	**Azione intrapresa per l'elaborazione dell'oggetto**
Nessun prefisso, virus di prova standard	Il file contiene un virus di prova. Non è possibili disinfettare l'oggetto.	L'applicazione identificherà l'oggetto come maligno, non lo sottoporrà a trattamento e lo eliminerà.

Prefisso	**Stato del virus di prova**	**Azione intrapresa per l'elaborazione dell'oggetto**
CORR–	Corrotto.	L'applicazione ha accesso al file ma non può farne la scansione, poichè l'oggetto è corrotto (per esempio la struttura del file è danneggiata o si tratta di un formato file non valido).
SUSP– WARN–	Il file contiene un test di prova (variante). Non è possibile disinfettare l'oggetto.	Questa è una variante del virus di prova. Al momento del rilevamento, l'applicazione non contiene nel suo database istruzioni su come trattare l'oggetto. Verrà quindi messo in quarantena e verrà analizzato nuovamente dopo l'aggiorna mento del database.
ERRO–	Errore in fase di elaborazione.	Si è verificato un errore durante l'analisi del file: l'applicazione non può evere accesso al file e non può effettuarne la scansione in quanto potrebbe essere stato violato (ad es., archivio multivolume senza fine) o non vi è alcun collegamento allo stesso (se ad esempio il file è su una risorsa di rete)
CURE–	Il file contiene un virus di prova. Può essere trattato. L'oggetto può essere sottoposto a scansione e il testo del codice del virus cambierà in `CURE`.	L'oggetto contiene un virus che può essere trattato. L'applicazione effettuerà una scansione del file e ne eliminerà il virus.
DELE–	Il file contiene un virus di prova. Non può essere disinfettatato.	L'oggetto contiene un virus che non può essere disinfettato o si tratta di un Trojan. L'applicazione eliminerà l'oggetto.

La prima colonna della tabella contiene i prefissi da aggiungere all'inizio della stringa del virus di prova standard. La seconda colonna descrive lo stato e la reazione di Kaspersky Internet Security ai vari tipi di virus di prova. La terza colonna invece contiene informazioni sulle azioni intraprese dal programma.

Le impostazioni scelte per il programma determinano l'azione che il programma effettuerà su ogni oggetto.

16.2. Test di File Anti-Virus

Per testare le funzionalità di File Anti-virus:

1. Consentire la notifica di tutti gli eventi in modo che il file del report contenga sia i dati sugli oggetti danneggiati che su quelli non scansionati a causa di errori. A tal fine, spuntare la voce **Registra eventi non critici** nella sezione **Report e file dati** nella finestra delle impostazioni del programma (vedi 19.3.1, p. 272).
2. Creare una cartella sul disco, copiare al suo interno il virus di prova scaricato dal sito EICAR (vedi 16.1 pag. 244) e le relative modifiche create.

File Anti-Virus rileverà i tentativi di accesso al file, ne effettuerà la scansione e informerà l'utente di aver rilevato un oggetto pericoloso:

Figura 82. Oggetto pericoloso rilevato

Una volta impostate le diverse azioni da intraprendere con gli oggetti rilevati, è possibile testare la reazione di File Anti-Virus al rilevamento di diversi tipi di oggetti.

E' possibile visualizzare i dettagli dell'attività di File Anti-Virus nel report del componente.

16.3. Test delle scansioni pianificate

Per testare le scansioni pianificate:

1. Creare una cartella sul disco, copiare al suo interno il virus di prova scaricato dal sito EICAR (vedi 16.1 pag. 244) e le relative modifiche create.
2. Creare una nuova attività di scansione (vedi 15.3, p. 230) e selezionare la cartella contenente i set di virus di prova come oggetti da sottoporre a scansione (16.1, p. 244).
3. Consentire la registrazione di tutti gli eventi nel file del report in modo che esso conservi sia i dati sugli oggetti danneggiati che su quelli non scansionati a causa di errori. A tal fine, spuntare la voce **Registra eventi non critici** nella sezione **Report e file dati** nella finestra delle impostazioni del programma (vedi 19.3.1, p. 272).
4. Effettuare l'attività di scansione anti-virus.

Quando si effettua la scansione, se vengono rilevati file sospetti o infetti, sullo schermo compariranno delle notifiche contenenti le informazioni sugli oggetti rilevati, chiedendo all'utente quale azione intraprendere:

Figura 83. Oggetto pericoloso rilevato

Tuttavia, selezionando diverse opzioni per le azioni, è possibile testare le reazioni di Kaspersky Internet Security al rilevamento di vari tipi di oggetti.

E' possibile vedere i dettagli dell'attività dell'antivirus nel report del componente.

CAPITOLO 17. AGGIORNAMENTI DEL PROGRAMMA

Mantenere aggiornato il software antivirus costituisce un investimento in termini di sicurezza per il proprio computer. Poiché ogni giorno nascono nuovi virus, trojan e altri software dannosi, per proteggere costantemente le proprie informazioni è fondamentale aggiornare regolarmente l'applicazione di protezione.

L'aggiornamento dell'applicazione implica lo scaricamento e l'installazione, sul proprio computer, dei seguenti componenti:

- **Database Antivirus, database Firewall e driver di rete**

  Per proteggere le informazioni presenti sul computer l'applicazione fa uso di definizioni dei virus e profili di attacchi di rete. I componenti del programma che forniscono la protezione utilizzano il database delle definizioni dei virus per rilevare e disinfettare oggetti dannosi eventualmente presenti. I database vengono aggiornati di ora in ora con la registrazione di nuove minacce e dei metodi per debellarle, ed è pertanto consigliabile aggiornarli in maniera regolare.

  In aggiunta alle definizioni di virus e al database degli attacchi ricevuti, vengono costantemente aggiornati anche i driver di rete che permettono ai componenti di protezione di intercettare il traffico di rete.

  Le precedenti versioni di applicazioni di Kaspersky Lab hanno supportato set di database *standard* ed e*stesi*, ciascuno dei quali proteggeva il computer da diversi tipi di oggetti pericolosi. Con Kaspersky Internet Security non è più necessario selezionare il set di database appropriato, poiché ora i prodotti utilizzano database che proteggono sia dal software nocivo che da riskware, oltre che dagli attacchi da parte di hacker.

- **Moduli dell'applicazione**

  Oltre ai database dell'applicazione, è possibile anche aggiornare i moduli di programma di Kaspersky Internet Security. Nuovi aggiornamenti dell'applicazione vengono elaborati con regolarità.

La principale fonte di aggiornamenti per Kaspersky Internet Security è rappresentata dai server di Kaspersky Lab. Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet.

E' necessario essere connessi ad Internet per poter scaricare gli aggiornamenti dai server. Nel caso in cui si disponesse di una connessione ad Internet attraverso un server proxy, è necessario configurare le impostazioni di connessione (vedi 19.7, p. 295)

Qualora non si disponesse di un accesso ai server di aggiornamento di Kaspersky Lab (ad esempio, se il computer non fosse connesso ad Internet), è possibile rivolgersi direttamente alla sede centrale di Kaspersky Lab chiamando il +7 (495) 797-87-00, +7 (495) 645-79-39 chiedendo di essere messi in contatto con partner di Kaspersky Lab che siano in grado di fornire gli aggiornamenti desiderati in formato compresso su floppy disk o CD/DVD.

Il download degli aggiornamenti può essere effettuato secondo una delle seguenti modalità:

- *Automatica*. Kaspersky Internet Security controlla le origini di aggiornamento a intervalli specificati per verificare la presenza di pacchetti di aggiornametno. Le scansioni possono essere impostate in modo da essere più frequenti in periodi di epidemie virali o meno frequenti dopo le stesse epidemie. Quando il programma rileva nuovi aggiornamenti, li scarica e li installa lsu computer. Questa è l'impostazione predefinita.
- *Pianificata*. L'aggiornamento è programmato in modo da cominciare ad un orario prestabilito.
- *Manuale*. Con questa opzione, la procedura di aggiornamento viene avviata manualmente.

Durante l'aggiornamento, l'applicazione confronta i database ed i moduli di programma presenti sul computer con le versioni disponibili sul server. Se il computer dispone delle versioni più recenti, la cosa verrà notificata in una apposita finestra, confermando che la macchina è aggiornata. Qualora le versioni presenti sul computer non corrispondano a quelle disponibili sul server, il programma eseguirà il download delle sole parti mancanti. Non verranno invece scaricati i database e i moduli già presenti sulla macchina, permettendo in tal modo un significativo aumento nella velocità del processo di aggiornamento ed una corrispondente riduzione del traffico in rete.

Prima di aggiornare i database, Kaspersky Internet Security ne esegue una copia di backup, che può essere utilizzata qualora fosse necessario tornare alla versione precedente (vedi 17.2 pag. 252). Nel caso in cui, ad esempio, il processo di aggiornamento danneggiasse i database rendendoli inutilizzabili, è possibile tornare facilmente alla versione precedente ed aggiornare i database in un momento successivo.

È possibile distribuire gli ultimi aggiornamenti su una risorsa locale durante l'aggiornamento dell'applicazione (vedi 17.3.3 pag. 257). Questa funzione

consente di aggiornare i database ed i moduli usati dalle applicazioni in versione 7.0 sui computer collegati in rete, risparmiando così ampiezza di banda.

17.1. Avvio della procedura di aggiornamento

È possibile iniziare l'aggiornamento in qualsiasi momento. Il processo opererà dall'origine dell'aggiornamento selezionata dall'utente (vedi 17.3.1 pag. 253).

La procedura di aggiornamento può essere avviata da:

- il menu contestuale (vedi 4.2 a pag. 53);
- la finestra principale dell'applicazione programma (vedi 4.3 a pag. 55).

Per avviare la procedura di aggiornamento dal menu di scelta rapida:

1. Aprire il menu di scelta rapida cliccando col pulsante destro del mouse sull'icona dell'applicazione nell'area di notifica della barra delle applicazioni.
2. Selezionare **Aggiornamento**.

Per avviare la procedura di aggiornamento dalla finestra principale del programma:

1. Aprire la finestra principale dell'applicazione e selezionare il componente **Aggiornamento**.
2. Fare clic sul link Aggiorna database.

Lo stato dell'aggiornamento verrà visualizzato nella finestra principale. Per conoscere i dettagli sul processo di aggiornamento, fare clic su Dettagli. Comparirà un report dettagliato dell'attività di scansione. la finestra del report può essere chiusa facendo clic su **Chiudi**. L'aggiornamento prosegue a finestra chiusa.

Notare che gli aggiornamenti sono distribuiti all'origine locale durante il processo di aggiornamento, a condizione che questa funzione sia abilitata (vedi 17.3.3 a pag. 257).

17.2. Ritorno all'aggiornamento precedente

Ogni volta che si avvia la procedura di aggiornamento, Kaspersky Internet Security crea innanzitutto una copia dei database e dei moduli dell'applicazione correnti, e solo successivamente inizia a scaricarne le nuove versioni. In tal modo, qualora l'aggiornamento non vada a buon fine, è possibile tornare ad utilizzare la versione precedente dei database.

Per ripristinare la versione precedente del database delle minacce note:

1. Aprire la finestra principale dell'applicazione e selezionare il componente **Aggiornamento**.
2. Cliccare su Ritorno ai database precedenti.

17.3. Configurazione delle impostazioni di aggiornamento

Le impostazioni della procedura di aggiornamento specificano i seguenti parametri:

- L'origine da cui l'aggiornamento viene scaricato e installato (vedi 17.3.1. pag. 253).
- La modalità di esecuzione della procedura di aggiornamento e degli specifici elementi aggiornati (vedi 17.3.2 pag. 255).
- La frequenza degli aggiornamenti programmati (vedi 6.7 pag. 79).
- L'account utente dal quale sarà eseguito l'aggiornamento (vedi 6.6 a pag. 78).
- Se gli aggiornamenti scaricati devono venir copiati su una directory locale (vedi 17.3.3 pag. 257).
- Le azioni da compiere al termine dell'aggiornamento (vedi 17.3.3 pag. 257).

Le seguenti sezioni prendono in esame gli aspetti sopra elencati.

17.3.1. Selezione di un'origine per l'aggiornamento

Per *origine degli aggiornamenti* si intende la risorsa contenente gli aggiornamenti dei database e dei moduli di Kaspersky Internet Security. Le origini degli aggiornamenti possono essere server HTTP e FTP, cartelle locali o cartelle di rete.

L'origine di aggiornamento principale è costituita dai *server degli aggiornamenti di Kaspersky Lab*. Si tratta di speciali siti web contenenti gli aggiornamenti disponibili per i database e i moduli delle applicazioni per tutti i prodotti Kaspersky Lab.

Se non si è in grado di accedere ai server degli aggiornamenti di Kaspersky Lab (per esempio perché manca la connessione Internet), è possibile rivolgersi alla sede di Kaspersky Lab chiamando il numero +7 (495) 797-87-00 per richiedere i nominativi dei partner Kaspersky Lab in grado di fornire gli aggiornamenti sotto forma di file compressi su dischetto o CD/DVD.

Attenzione!

Per richiedere gli aggiornamenti su supporti rimovibili, è necessario specificare se si desiderano anche gli aggiornamenti dei moduli dell'applicazione.

È possibile copiare gli aggiornamenti da un disco e caricarli su un sito FTP o HTTP oppure salvarli in una cartella locale o di rete.

Selezionare l'origine degli aggiornamenti nella scheda **Origine aggiornamento** (vedi Figura 84).

Per impostazione predefinita, gli aggiornamenti sono scaricati dai server degli aggiornamenti di Kaspersky Lab. L'elenco dei server non può essere modificato. Durante l'aggiornamento, Kaspersky Internet Security consulta l'elenco, seleziona l'indirizzo del primo server e cerca di scaricare i file. Se il download dei file dal primo server non va a buon fine, l'applicazione cerca di connettersi al server successivo e di scaricare i file da quello, e così via, fino ad esito positivo dell'operazione.

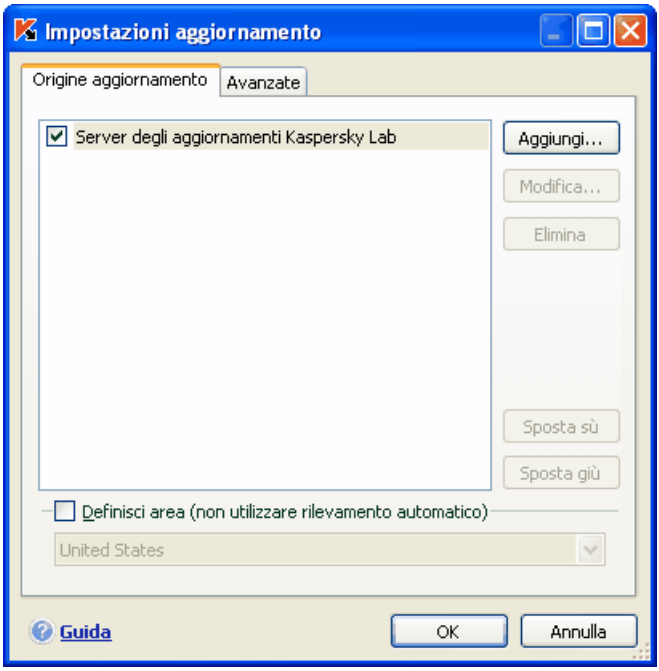


Figura 84. Selezione di un'origine di aggiornamento

Per scaricare gli aggiornamenti da un altro sito FTP o HTTP:

1. Fare clic su **Aggiungi**.
2. Nella finestra di dialogo **Seleziona origine aggiornamento**, selezionare il sito FTP o HTTP o specificare l'indirizzo IP, il nome o l'indirizza URL di questo sito nel campo **Origine**. Quando si seleziona un sito ftp come origine dell'aggiornamento, le impostazioni di autenticazione devono essere digitate nell'URL del server nel formato ftp://userpassword@server.

Attenzione!

Se come origine degli aggiornamenti è stata selezionata una risorsa esterna alla LAN è necessaria una connessione Internet per scaricare i file.

Per scaricare l'aggiornamento da una cartella locale:

1. Fare clic su **Aggiungi**.

2. Nella finestra di dialogo **Seleziona origine aggiornamento**, selezionare una cartella o specificare il percorso completo di questa cartella nel campo **Origine**.

Kaspersky Internet Security aggiunge la nuova origine all'inizio dell'elenco e la abilita automaticamente spuntando la casella vicino al nome.

Se sono state selezionate più risorse, l'applicazione cerca di connettersi ad esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco, e preleva gli aggiornamenti dalla prima disponibile. È possibile modificare l'ordine delle origini nell'elenco servendosi dei pulsanti **Sposta su** e **Sposta giù**.

Per modificare l'elenco, usare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. L'unico tipo di origine che non può essere modificato né eliminato sono i server degli aggiornamenti di Kaspersky Lab.

Se si prelevano gli aggiornamenti dai server di Kaspersky Lab, è possibile selezionare la posizione ottimale del server da cui scaricare i file. Kaspersky Lab dispone di server in diversi paesi. La scelta del server di Kaspersky Lab più vicino aiuta a risparmiare tempo e ad accelerare il prelievo degli aggiornamenti.

Per scegliere il server più vicino, selezionare la casella **Definisci area (non utilizzare rilevamento automatico)** e selezionare quindi dall'elenco a discesa il paese più vicino al proprio paese di residenza. Spuntando questa casella gli aggiornamenti terranno conto della regione selezionata nell'elenco. Questa casella è per impostazione deselezionata e viene utilizzata l'informazione contenuta nel registro di sistema.

17.3.2. Selezione di un metodo di aggiornamento e degli oggetti da aggiornare

Durante la configurazione delle impostazioni di aggiornamento è importante definire cosa sarà aggiornato e con quale metodo.

Le impostazioni di aggiornamento (vedi Figura 85) definiscono i componenti che si desidera aggiornare:

- Database dell'applicazione.
- Driver di rete che abilitano i componenti di protezione ad intercettare il traffico di rete.
- Database del Firewall contenete la descrizione degli attacchi di rete.
- Moduli del programma.

I database dell'applicazione, i driver di rete ed il database del Firewall sono sempre aggiornati mentre i moduli dell'applicazione vengono aggiornati solo se le loro impostazioni lo prevedono.

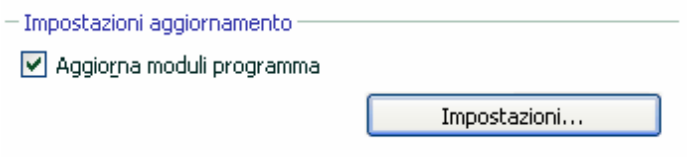


Figura 85. Selezione degli oggetti da aggiornare

Se si desidera scaricare e installare gli aggiornamenti dei moduli del programma:

Aprire la finestra delle impostazioni dell'applicazione, fare clic su **Aggiornamento** e selezionare la casella **Aggiorna moduli programma**.

Se nell'origine prescelta è disponibile un aggiornamento dei moduli del programma, l'applicazione scaricherà i database necessari e li applicherà dopo il riavvio del sistema. Gli aggiornamenti dei moduli scaricati non saranno installati fino apparirà al riavvio del computer.

La modalità di esecuzione (vedi Figura 86) definisce le modalità di avvio del tool di aggiornamento. È possibile selezionare una delle seguenti opzioni:

Automatica. Selezionando questa opzione, Kaspersky Internet Security controlla le origini a intervalli definiti per verificare la presenza di aggiornamento (vedi 17.3.1 a pag. 253). Quando il programma rileva nuovi aggiornamenti, li scarica e li installa sul computer. Questa modalità è selezionata per impostazione predefinita.

Se come origine di aggiornamento è specificata una risorsa di rete, Kaspersky Internet Security cerca di lanciare l'aggiornamento ogni volta che il computer si connette a quella risorsa o dopo che è trascorso un certo periodo di tempo come specificato nel precedente pacchetto di aggiornamento. Se come origine di aggiornamento è stata selezionata una cartella locale, l'applicazione cerca di scaricare gli aggiornamenti da quest'ultima con la frequenza specificata nell'ultimo pacchetto di aggiornamento scaricato. Questa opzione consente a Kaspersky Lab di regolare la frequenza di aggiornamento del programma in caso di epidemie o di altre situazioni potenzialmente pericolose. L'applicazione riceverà tempestivamente gli aggiornamenti più recenti dei database e dei moduli dell'applicazione, impedendo ai programmi nocivi di penetrare nel computer.

Figura 86. Selezione di una modalità di esecuzione degli aggiornamenti

Ogni 1 giorno. L'aggiornamento è programmato per avviarsi a un'ora specificata. La frequenza predefinita è una volta al giorno. Per modificare la programmazione predefinita, fare clic sul pulsante **Cambia…** nella sezione della modalità di esecuzione e apportare le modifiche desiderate nella finestra che si apre (per ulteriori informazioni, vedi 6.7 a pag. 79).

Manuale. Questa opzione consente di avviare l'aggiornamento manualmente. Kaspersky Internet Security informa l'utente quando è necessario provvedere all'aggiornamento.

17.3.3. Distribuzione dell'aggiornamento

Se i computer di casa sono connessi attraverso una rete domestica, non occorre scaricare ed installare gli aggiornamenti su ciascuno di essi separatamente, in quanto consumeresti più banda del necessario. È possibile usare la funzione di distribuzione dell'aggiornamento che aiuta a ridurre il traffico recuperando gli aggiornamenti nel modo seguente:

1. Uno dei computer della rete recupera un pacchetto di aggiornamento dai server di Kaspersky Lab o da una altra risorsa web contenente gli ultimi aggiornamenti. Gli aggiornamenti così recuperati vengono posti in una cartella ad accesso pubblico.
2. Gli altri computer della rete accedono a questa cartella per recuperare gli aggiornamenti.

Per abilitare la distribuzione degli aggiornamenti spuntare la casella **Aggiornare cartella di distribuzione** nella scheda **Avanzate** (vedi Figura 87) e nel campo sottostante specificare la cartella condivisa in cui verranno posti gli aggiornamenti. È possibile inserire manualmente il percorso o selezionarla cliccando su **Sfoglia** nella finestra che si apre. Se la casella è selezionata gli aggiornamenti verranno automaticamente copiati in essa non appena recuperati.

Notare che Kaspersky Internet Security 7.0 recupera dai server di aggiornamento di Kaspersky Lab solo i pacchetti degli aggiornamenti per la versione v. 6.0

Affinché gli altri computer della rete possano scaricare gli aggiornamenti dalla cartella condivisa, eseguire i passaggi seguenti:

1. Assicurare l'accesso pubblico a questa cartella.
2. Specificare la cartella condivisa come origine degli aggiornamenti nelle impostazioni del modulo di aggiornamento.

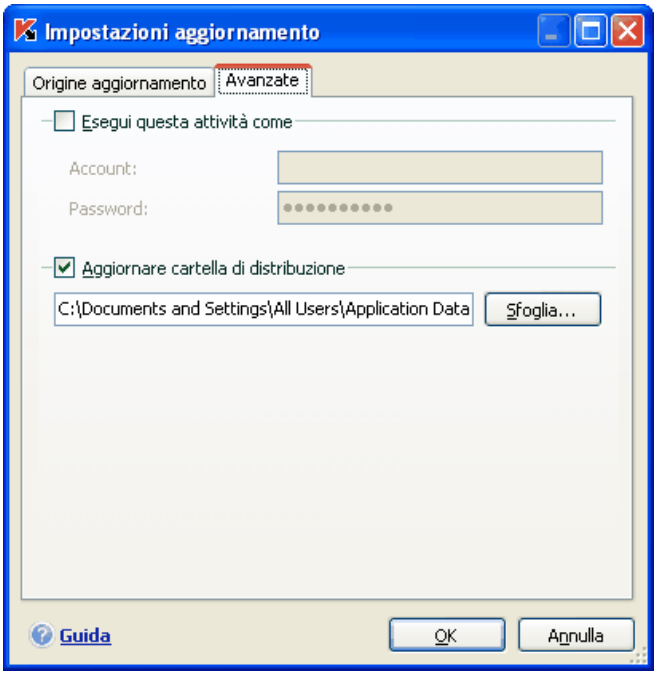


Figura 87. Impostazioni strumento per la copia degli aggiornamenti

17.3.4. Azioni successive all'aggiornamento del programma

Ogni aggiornamento dei database contiene nuovi elementi che proteggono il computer dalle minacce più recenti.

Kaspersky Lab raccomanda di esaminare ogni volta gli *oggetti in quarantena* e gli *oggetti di avvio* dopo l'aggiornamento del database.

Perché è necessario esaminare questi oggetti?

La cartella Quarantena contiene oggetti che il programma ha catalogato come sospetti o potenzialmente infetti (vedi 19.1 pag. 263). Utilizzando la versione più recente dei database, Kaspersky Internet Security potrebbe essere in grado di identificare la minaccia e di eliminarla.

Per impostazione predefinita, l'applicazione esamina gli oggetti in quarantena dopo ogni aggiornamento dei database. Si raccomanda inoltre di consultare periodicamente gli oggetti in quarantena poiché il loro stato può cambiare dopo molte scansioni. Alcuni oggetti possono quindi essere ripristinati nelle posizioni originarie e può essere possibile continuare a lavorare con loro.

Per disabilitare la scansione degli oggetti in Quarantena, deselezionare la casella **Ripeti scansione Quarantine** nella sezione **Azione post-aggiornamento**.

Gli oggetti di avvio sono di importanza vitale per la sicurezza del computer. Se uno di essi è infetto da un'applicazione nociva, potrebbe verificarsi un errore di avvio del sistema operativo. Kaspersky Internet Security è dotato di un'attività di scansione degli oggetti di avvio per questa area (vedi Capitolo 14 pag. 215). Si raccomanda di pianificare un calendario di esecuzione per questa attività in modo da avviarlo automaticamente ad ogni aggiornamento dei database (vedi 6.7 pag. 79).

CAPITOLO 18. GESTIONE DELLE CHIAVI

Kaspersky Internet Security necessita di un *file chiave* per funzionare, che viene fornito all'acquisto del programma. Tale chiave assicura il diritto di utilizzare il programma dal giorno dell'installazione.

Senza la chiave, a meno che non sia stata attivata una versione di prova del programma, Kaspersky Internet Security opererà in una sola modalità di aggiornamento. Il programma non scaricherà alcun nuovo aggiornamento disponibile.

Se è stata attivata la versione di prova del programma, al termine del periodo di prova, Kaspersky Internet Security non funzionerà più.

Allo scadere della chiave acquistata, il programma continuerà a funzionare ma non sarà possibile aggiornare i database dell'applicazione. Il computer continuerà ad essere scansionato e protetto dai componenti di protezione ma con database aggiornati al momento della scadenza della chiave. Non possiamo garantire la protezione dai virus generati dopo la scadenza della chiave.

Per evitare che il computer venga infettato da nuovi virus consigliamo di estendere la validità della chiave. Il programma segnalerà all'utente due settimane prima il termine di validità della chiave e in questo periodo il messaggio verrà visualizzato ad ogni avvio dell'applicazione.

Le informazioni circa la chiave corrente sono mostrate sotto **Attivazione** (vedi Figura 88) nella finestra principale dell'applicazione. La sezione **Chiave installata** mostra l'ID della chiave, il tipo (retail, di prova, per i beta test), numero di host su cui installarla, data di scadenza e numero di giorni prima della scadenza. Cliccare su Informazioni dettagliate della chiave per ulteriori informazioni.

Per vedere le clausole del contratto di licenza cliccare su Visualizza contratto di licenza con l'utente finale. Per rimuovere una chiave dall'elenco cliccare su Elimina Chiave.

Per acquistare o rinnovare una chiave:

1. Acquistare una nuova chiave cliccando su Acquista chiave (l'applicazione non è stata attivata) oppure Estendi la chiave. La corrispondente pagina web conterrà tutte le informazioni per comprare una chiave online sul sito di Kaspersky Lab o da un suo partner aziendale.

Acquistando online una chiave o un codice di attivazione, questi saranno inviati via posta elettronica all'indirizzo specificato nel modulo d'ordine non appena eseguito il pagamento.

2. Installa la chiave cliccando Installa chiave sotto **Attivazione** nella finestra principale di Kaspersky Internet Security o **Attivazione** nel menu contestuale. Verrà avviata la procedura guidata di attivazione (vedi 3.2.2 pag. 40).

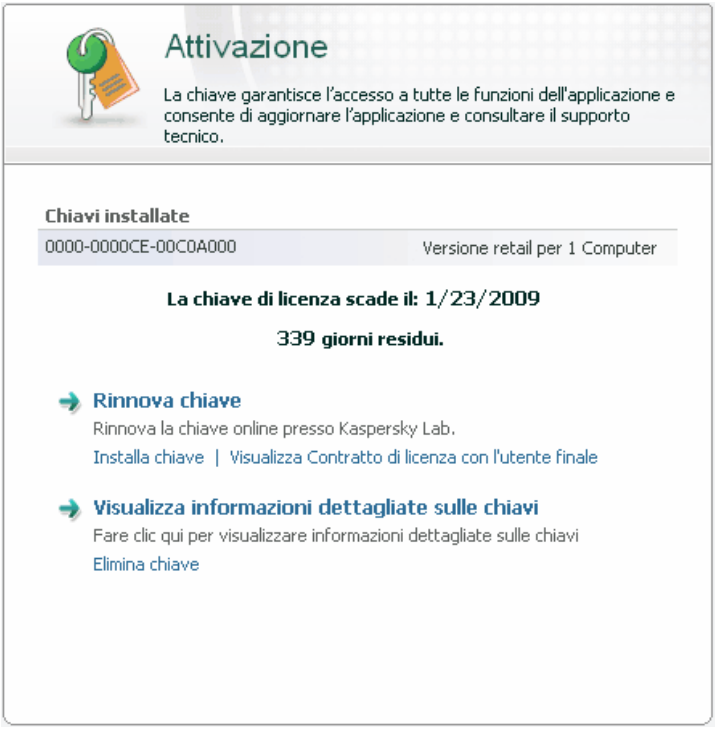


Figura 88. Gestione della chiave

Kaspersky Lab mette a punto regolarmente offerte speciali per l'estensione della licenza dei propri prodotti. Controllare sul sito Kaspersky Lab nell'area **Prodotti → Vendita ed offerte speciali**.

CAPITOLO 19. OPZIONI AVANZATE

Kaspersky Internet Security è dotato di funzioni avanzate che ne espandono la funzionalità.

Il programma colloca alcuni oggetti in apposite aree di archiviazione al fine di garantire la massima protezione dei dati riducendo al minimo le perdite.

- La cartella Backup contiene copie degli oggetti modificati o eliminati da Kaspersky Internet Security (vedi 19.2 pag. 267) Se un oggetto conteneva informazioni importanti e non è stato possibile recuperarlo completamente durante l'elaborazione antivirus, è possibile ripristinare l'oggetto dalla copia di backup.

- La Quarantena contiene oggetti potenzialmente infetti che non è stato possibile elaborare con i database correnti dell'applicazione (vedi 19.1 pag. 263).

Si raccomanda di esaminare periodicamente l'elenco degli oggetti memorizzati in tali aree. Alcuni di essi infatti possono essere già obsoleti e altri possono essere stati ripristinati.

Alcune funzioni sono state ideate per aiutare l'utente durante l'uso del programma. Ad esempio:

- Il servizio di Supporto Tecnico offre un'assistenza completa per Kaspersky Internet Security (vedi 19.10 pag. 308). Kaspersky offre una scelta di canali di supporto più vasta possibile: assistenza on-line, forum degli utenti e conoscenze di base.

- La funzione di Notifica serve per configurare le notifiche agli utenti relative a eventi chiave di Kaspersky Internet Security (vedi 19.9.1 pag. 301). Può trattarsi di eventi di natura informativa o di errori da eliminare immediatamente, ed è estremamente importante esserne a conoscenza.

- La funzione di Auto-Difesa protegge i file del programma da qualsiasi modifica o danno perpetrati dagli hacker, blocca l'uso delle funzioni del programma da parte di amministrazioni remote e proibisce ad altri utenti del computer di eseguire determinate azioni in Kaspersky Internet Security (vedi 19.9.1.3 pag. 304). Per esempio, la modifica del livello di protezione può influire considerevolmente sulla sicurezza del computer.

- La Gestione della configurazione dell'applicazione archivia i parametri di funzionamento dell'applicazione e facilita la replica di tali parametri su

altri computer (vedi 19.9.3 pag 307) come pure un ripristino delle impostazioni predefinite (vedi 19.9.4 pag. 307).

Il programma offre anche dettagliati report (vedi 19.3 pag. 269) sul funzionamento di tutti i componenti di protezione, attività di scansione antivirus ed aggiornamenti.

Il monitoraggio delle porte può regolare quali moduli controllano i dati trasferiti sulle porte stesse (vedi 19.5 pag. 291). La configurazione delle impostazioni del server proxy (vedi 19.7 pag. 295) assicura l'accesso dell'applicazione ad Internet che è critica per alcuni componenti di protezione in tempo reale e per gli aggiornamenti.

Il disco di emergenza può agevolare il ripristino della funzionalità del computer dopo un'infezione (vedi 19.4 pag. 287). Si tratta di una funzione particolarmente utile quando non si riesce a caricare il sistema operativo del computer in seguito al danneggiamento dei file system parte di un codice nocivo.

È possibile inoltre modificare l'aspetto di Kaspersky Internet Security e personalizzare l'interfaccia del programma (vedi 19.7 pag. 295).

Di seguito esaminiamo in dettaglio queste funzioni.

19.1. Quarantena per gli oggetti potenzialmente infetti

La **Quarantena** è una speciale area di archiviazione che contiene gli oggetti potenzialmente infetti.

Gli **oggetti potenzialmente infetti** sono oggetti sospettati di contenere un virus o la variante di un virus.

Perché *potenzialmente infetti*? Non sempre è possibile stabilire con certezza se un oggetto sia infetto oppure no. Questo è dovuto a diverse ragioni:

- *Il codice dell'oggetto esaminato somiglia a una minaccia nota ma appare parzialmente modificato.*

  I database dell'applicazione contengono minacce già studiate da Kaspersky Lab. Se un programma nocivo è stato modificato e le variazioni non sono ancora state registrate nei database, Kaspersky Internet Security classifica l'oggetto contenente il programma nocivo modificato come potenzialmente infetto e indica la minaccia a cui il codice somiglia.

- *Il codice dell'oggetto intercettato ricorda per struttura un programma nocivo.* Tuttavia nessun oggetto simile è ancora registrato nei database.

È possibile che si tratti di un nuovo tipo di minaccia, perciò Kaspersky Internet Security classifica l'oggetto come potenzialmente infetto.

L'analizzatore del *codice euristico* intercetta i virus potenziali. Questo meccanismo è abbastanza efficace e molto raramente produce un falso positivo.

Un oggetto potenzialmente infetto può essere intercettato e trasferito in Quarantena da File Anti-Virus, Mail Anti-Virus , Difesa proattiva o nel corso di una scansione antivirus.

Per mettere un oggetto in quarantena, cliccare su Quarantena nella notifica che compare al rilevamento di un oggetto potenzialmente infetto.

Quando un oggetto viene messo in Quarantena, esso non viene copiato ma trasferito. L'oggetto viene quindi eliminato dal disco o dall'e-mail e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in uno speciale formato e pertanto non sono pericolosi.

19.1.1. Azioni da eseguire sugli oggetti in Quarantena

Il numero totale degli oggetti presenti nella cartella **Quarantena** è visualizzato nella sezione **Report e file dati** della finestra principale. Nella parte destra dello schermo si trova una speciale sezione *Quarantena* che indica:

- Il numero dei file potenzialmente infetti intercettati da Kaspersky Internet Security;
- le dimensioni correnti della cartella Quarantena.

Da qui è possibile eliminare tutti gli oggetti in Quarantena per mezzo del pulsante Elimina.

Per accedere agli oggetti in Quarantena:

Cliccare Quarantena.

Nella scheda **Quarantena** (vedi Figura 89) è possibile compiere le seguenti azioni:

- Trasferire in Quarantena un file sospettato di contenere un'infezione che il programma non ha rilevato. A tal fine, cliccare su **Aggiungi** e selezionare il file desiderato nella finestra di selezione. Il file viene aggiunto all'elenco con lo stato *Aggiunto dall'utente*.
- Esaminare e riparare tutti gli oggetti potenzialmente infetti in Quarantena per mezzo delle versione corrente dei database dell'applicazione facendo clic su **Scansione completa**.

Dopo la scansione e l'eventuale riparazione di oggetti in Quarantena, il loro stato può cambiare in *infetto, potenzialmente infetto,falso positivo, OK* ecc.

Lo stato *infetto* significa che l'oggetto è stato riconosciuto come infetto ma non è stato possibile ripararlo. Si raccomanda di eliminare gli oggetti appartenenti a questa categoria.

Tutti gli oggetti classificati come *falso positivo* possono essere ripristinati poiché il precedente stato di *potenzialmente infetto* non è stato confermato dal programma in seguito alla nuova scansione.

- Ripristinare i file in una cartella selezionata dall'utente o nella cartella in cui si trovavano prima della Quarantena (impostazione predefinita). Per ripristinare un oggetto, selezionarlo dall'elenco e fare clic su **Ripristina**. Durante il ripristino di oggetti da archivi, database di posta e file in formato posta trasferiti in Quarantena, è necessario selezionare anche la directory in cui ripristinarli.

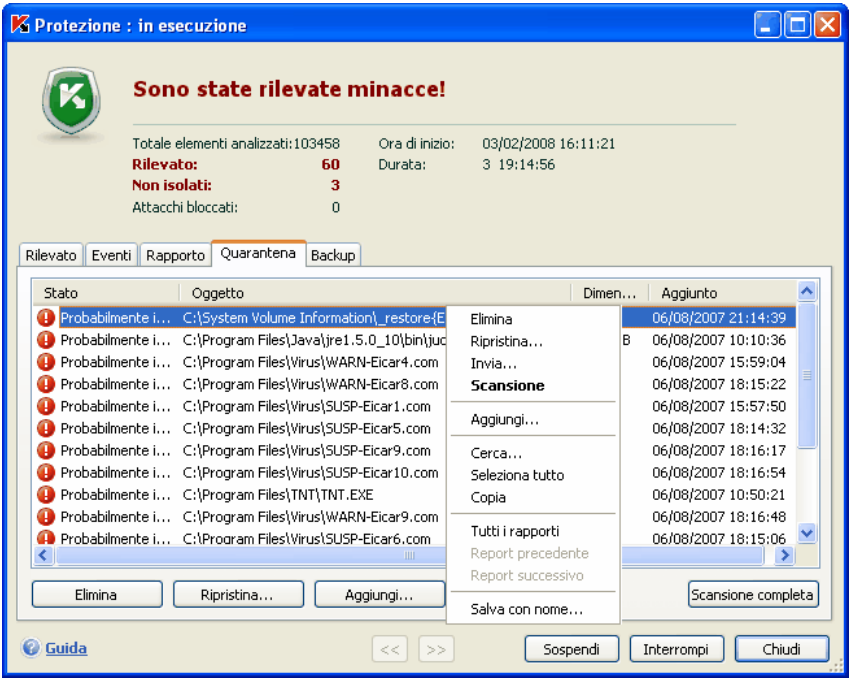


Figura 89. Elenco degli oggetti in Quarantena

Suggerimento:

Si raccomanda di ripristinare solo gli oggetti classificati come *falso positivo, OK* e *disinfettato* poiché il ripristino di altri oggetti può provocare l'infezione del computer.

- Eliminare oggetti o gruppi selezionati di oggetti in Quarantena. Eliminare solo gli oggetti che non possono essere riparati. Per eliminare questi oggetti, selezionarli nell'elenco e fare clic su **Elimina**.

19.1.2. Configurazione della Quarantena

È possibile configurare le impostazioni di layout e funzionamento dell'area Quarantena, in particolare:

- Impostare scansioni automatiche di oggetti in Quarantena dopo ogni aggiornamento dei database dell'applicazione (per ulteriori informazioni vedi 17.3.3 pag. 257).

Attenzione!

Se si sta accedendo all'area Quarantena, il programma non è in grado di esaminare gli oggetti subito dopo l'aggiornamento dei database.

- Impostare la durata massima della memorizzazione degli oggetti in Quarantena.

  La durata predefinita è di 30 giorni, allo scadere dei quali gli oggetti vengono eliminati. È possibile modificare la durata di memorizzazione in Quarantena o disabilitare del tutto questa limitazione.

A tal fine:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Report e file dati**.
2. Nella sezione **Quarantena Backup** (vedi Figura 90) digitare il tempo massimo allo scadere del quale gli oggetti saranno automaticamente eliminati. In alternativa deselezionare la casella per disabilitare l'eliminazione automatica.

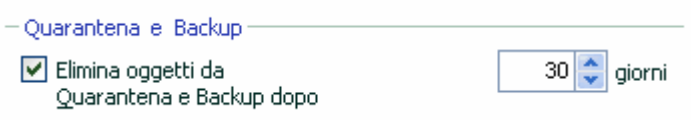


Figura 90. Configurazione del periodo di memorizzazione degli oggetti in Quarantena

19.2. Copie di Backup di oggetti pericolosi

A volte, in seguito alla riparazione, gli oggetti perdono la propria integrità. Se un file riparato contiene informazioni importanti e dopo la riparazione risulta parzialmente o completamente danneggiato, si può tentare di ripristinare l'oggetto originario da una copia di backup.

Una **copia di backup** è una copia dell'oggetto pericoloso creata prima di riparare o eliminare l'originale. Le copie di backup vengono salvate nella cartella Backup.

La cartella **Backup** è una particolare area di archiviazione che contiene copie di oggetti pericolosi da riparare o eliminare. I file in Backup vengono salvati in uno speciale formato e pertanto non sono pericolosi.

19.2.1. Azioni da eseguire sulle copie di backup

Il numero totale delle copie di backup a disposizione è visualizzato nella sezione **Report e File dati** della finestra principale. Nella parte destra dello schermo si trova uno speciale riquadro **Backup** che indica:

- Il numero di copie di backup degli oggetti create da Kaspersky Internet Security;
- le dimensioni correnti della cartella Backup.

Da qui è possibile eliminare tutte le copie di backup per mezzo del link **Cancella**.

Per accedere alle copie di oggetti pericolosi:

Cliccare su Backup.

Viene visualizzato un elenco di copie di backup nella scheda **Backup** (vedi Figura 91). Per ogni copia sono fornite le seguenti informazioni: il percorso completo ed il nome dell'oggetto, lo stato dell'oggetto assegnato dalla scansione e le sue dimensioni.

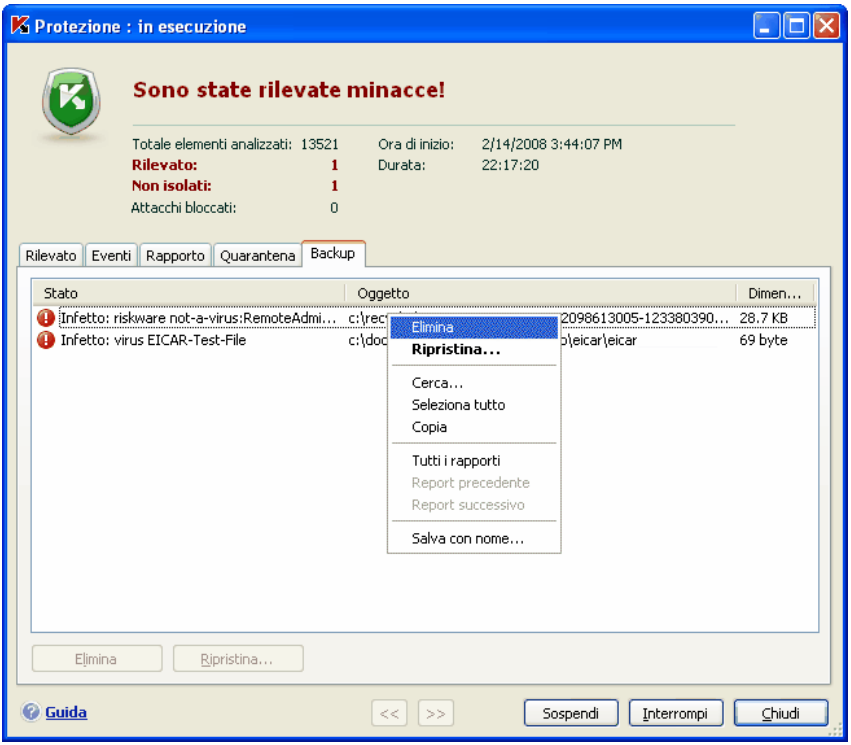


Figura 91. Copie di backup di oggetti eliminati o disinfettati

È possibile ripristinare le copie selezionate per mezzo del pulsante **Ripristina**. L'oggetto viene così ripristinato dalla cartella Backup con lo stesso nome dell'originale prima della riparazione.

Se esiste già un oggetto con quel nome nella posizione originaria (ciò è possibile se prima della riparazione è stata creata una copia dell'oggetto che si desidera ripristinare), viene visualizzato un apposito messaggio. È possibile quindi cambiare posizione all'oggetto da ripristinare oppure rinominarlo.

Si raccomanda di sottoporre l'oggetto a scansione antivirus subito dopo il ripristino. È possibile che i database aggiornati dell'applicazione consentano di ripulirlo senza perdere l'integrità del file.

Si consiglia di ripristinare le copie di backup degli oggetti solo se strettamente necessario. Ciò potrebbe provocare l'infezione del computer.

Si raccomanda di esaminare periodicamente la cartella Backup e di vuotarla servendosi del pulsante **Elimina**. È possibile inoltre configurare il programma in

modo da eliminare automaticamente dal Backup le copie di più vecchia data (vedi 19.2.2 pag. 269).

19.2.2. Configurazione delle impostazioni del Backup

È possibile definire la durata massima di conservazione nella cartella Backup.

La durata predefinita è di 30 giorni, allo scadere dei quali le copie vengono eliminate. È possibile inoltre modificare la durata di conservazione o disabilitare del tutto questa limitazione procedendo come segue:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Report e file dati**.
2. Impostare la durata della conservazione delle copie di backup nella sezione **Quarantena Backup** (vedi Figura 90) nella parte destra della finestra. In alternativa, deselezionare la casella per disabilitare l'eliminazione automatica.

19.3. Report

Le azioni dei componenti di Kaspersky Internet Security e le attività di scansione antivirus sono registrate in appositi report.

Il numero totale dei report creati dal programma in un certo momento e le loro dimensioni totali in bite sono visualizzati nella sezione **Report e File dati** nella finestra principale del programma. Queste informazioni sono presentate nella sezione **Rapporto**.

Per visualizzare i report:

Cliccare su **Rapporto**.

La scheda **Rapporto** (vedi Figura 92) elenca i report più recenti di tutti i componenti, le attività di scansione e degli aggiornamenti eseguite durante la sessione corrente di Kaspersky Internet Security. Il loro stato è indicato vicino a ciascun componente od azione: per esempio, *in esecuzione, sospeso o completato*. Se si desidera visualizzare la cronologia completa della creazione dei report per la sessione corrente del programma, selezionare la casella **Mostra cronologia rapporto**.

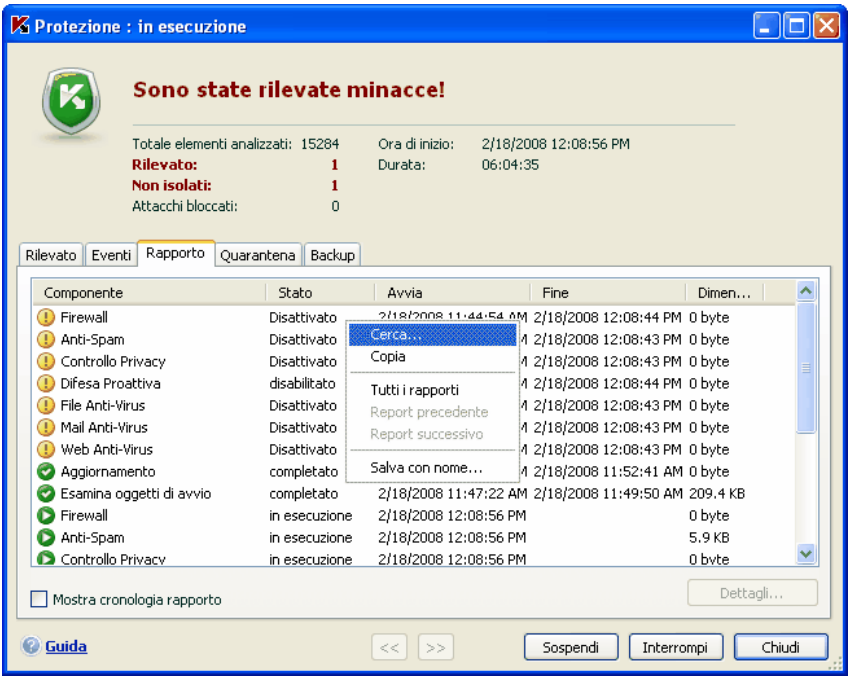


Figura 92. Report sul funzionamento dei componenti

Per consultare tutti gli eventi registrati nel report di un componente o attività:

Selezionare il nome del componente o attività nella scheda **Rapporto** e fare clic sul pulsante **Dettagli**.

Si apre una finestra contenente informazioni dettagliate sulle prestazioni del componente o attività selezionati. Le statistiche sulle prestazioni sono visualizzate nella parte superiore della finestra, mentre le informazioni dettagliate sono riportate nelle schede. Le schede sono diverse a seconda del componente o attività:

- La scheda **Rilevato** contiene un elenco di oggetti pericolosi individuati da un componente o da un'attività di scansione antivirus.
- La scheda **Eventi** visualizza gli eventi relativi al componente o attività.
- La scheda **Statistiche** contiene le statistiche dettagliate su tutti gli oggetti esaminati.
- La scheda **Impostazioni** visualizza le impostazioni utilizzate da componenti di protezione, scansioni antivirus o aggiornamenti dei database.

- Le schede **Registro** sono presenti solo nel report di Difesa proattiva e contengono informazioni su tutti i tentativi di modificare il registro del sistema operativo.
- Le schede **Siti di Phishing, Tentativi di connessione**, **Tentativi di trasmissione dati** si trovano solo nel report di Controllo Privacy.
- Le schede **Attacchi provenienti dalla rete, Lista di macchine con accesso bloccato, Attività applicazione, Filtri Pacchetti, Popup** e **Banner** sono solo nel report del Firewall. Essi comprendono le informazioni circa tutti i tentativi di attacco ala rete sul computer dell'utente, host banditi dopo l'attacco, descrizione dell'attività di rete dell'applicazione che corrisponde alle regole esistenti e tutti i pacchetti di dati che corrispondono alle regole di filtro pacchetti del Firewall.
- Le schede **Connessioni stabilite, Porte aperte** e **Traffico** coprono anch'esse l'attività di rete sul tuo computer mostrando le connessioni correnti, le porte aperte e la quantità di traffico che il computer ha inviato o ricevuto.

I report possono essere interamente esportati in formato testo. Questa funzione è utile nei casi in cui in un componente o attività si sia verificato un errore impossibile da eliminare autonomamente, per il quale si necessita di assistenza tecnica. In tali casi è necessario inviare il report in formato .txt al servizio di Supporto Tecnico tecnica per consentire ai nostri specialisti di studiare approfonditamente il problema e risolverlo nel più breve tempo possibile.

Per esportare un report in formato testo:

Cliccare su **Azione** → **Salva con nome** e specificare dove salvare il file del report.

Al termine del lavoro con il report, fare clic su **Chiudi**.

Esiste un pulsante **Azioni** su tutte le schede ad eccezione di **Impostazioni** e **Statistiche**, che può essere utilizzato per definire le reazioni agli oggetti presenti nell'elenco. Facendo clic su di esso, si apre un menu contestuale con i seguenti elementi di menu (il menu è diverso a seconda del componente; di seguito sono elencate tutte le opzioni possibili):

Disinfetta – il programma cerca di riparare l'oggetto pericoloso. Puoi lasciarlo nell'elenco per scansionarlo in seguito con database aggiornati o cancellarlo. Puoi applicare questa azione ad un singolo oggetto o a molti degli oggetti elencati

Elimina gli oggetti pericolosi dal computer.

Elimina dall'elenco – elimina il record dell'oggetto riconosciuto dal report

Aggiungi a zona attendibile – l'oggetto viene escluso dalla protezione. Si apre una finestra con una regola di esclusione per l'oggetto.

Vai a file – si apre la cartella in cui è stato salvato l'oggetto in Microsoft Windows Explorer.

Neutralizza tutti – tutti gli oggetti presenti nell'elenco vengono neutralizzati. Kaspersky Internet Security cerca di elaborare gli oggetti per mezzo dei database dell'applicazione.

Pulisci tutti – il report sugli oggetti rilevati viene azzerato. Con questa funzione, tutti gli oggetti pericolosi rilevati restano nel computer.

Cerca www.viruslist.com – vengono cercate le descrizioni dell'oggetto nell'Enciclopedia dei Virus nel sito web di Kaspersky Lab.

Cerca – consente di inserire caratteri di ricerca per nome o stato degli oggetti in elenco.

Salva con nome – salva il report come file testo.

Inoltre è possibile organizzare le informazioni visualizzate in ordine crescente o decrescente per ciascuna colonna cliccando sull'intestazione della colonna.

Per elaborare gli oggetti pericolosi riconosciuti da Kaspersky Internet Security premere il pulsante **Neutralizza** (per un oggetto o gruppo di oggetti) o **Neutralizza Tutto** (per processare tutti gli oggetti dell'elenco). Dopo che ogni oggetto è stato elaborato apparirà un messaggio sullo schermo. A questo punto occorre decidere cosa fare con gli stessi in seguito.

Se si spunta **Applica a tutti** nella finestra di notifica l'azione scelta verrà applicata a tutti gli oggetti con lo stato selezionato dall'elenco prima di essere elaborati.

19.3.1. Configurazione delle impostazioni dei report

Per configurare le impostazioni di creazione e salvataggio dei report:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Report e File dati**.
2. Modificare le impostazioni sotto **Report** (vedi Figura 93) come segue:
   - Consentire o disabilitare la registrazione di eventi informativi. Questi eventi di solito non sono rilevanti ai fini della sicurezza. Per registrare gli eventi, selezionare la casella **Registra eventi non critici**.
   - Scegliere di salvare nel report solo gli eventi verificatisi successivamente all'ultima scansione. Questa impostazione consente di risparmiare spazio su disco riducendo le dimensioni del report. Se la casella **Mantieni solo eventi recenti** è

selezionata, il report si creerà da zero ogni volta che si riavvia l'attività. Tuttavia saranno sovrascritte solo le informazioni non critiche.

- Impostare la durata della conservazione dei report. La durata predefinita è di 30 giorni, allo scadere dei quali i report vengono eliminati. È possibile modificare la durata massima di conservazione o disabilitare del tutto questa limitazione.

Figura 93. Configurazione delle impostazioni dei report

19.3.2. La scheda *Rilevato*

Questa scheda (vedi Figura 94) contiene un elenco di oggetti pericolosi rilevati da Kaspersky Internet Security. Per ogni oggetto è indicato il nome completo, accompagnato dallo stato assegnatogli dal programma in seguito alla scansione o all'elaborazione.

Se si desidera che l'elenco contenga sia gli oggetti pericolosi sia quelli neutralizzati con successo, selezionare la casella **Mostra oggetti disinfettati**.

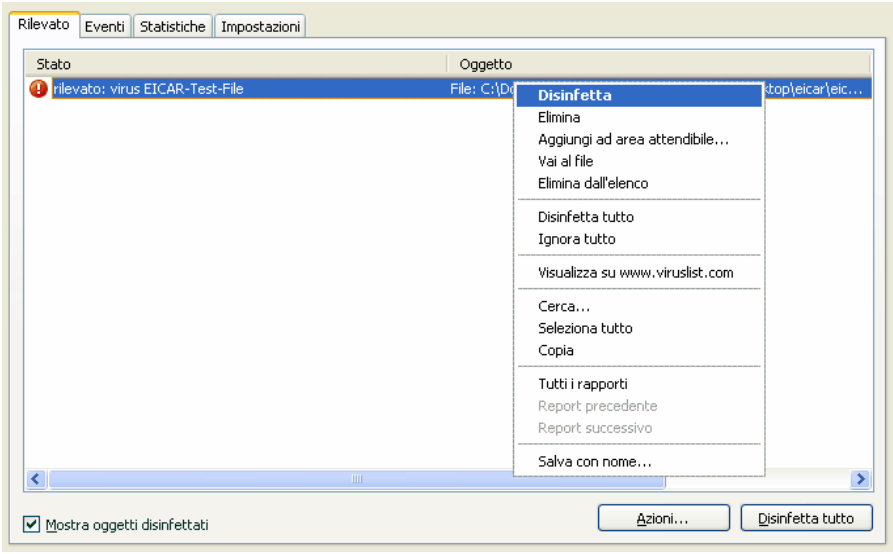


Figura 94. Elenco degli oggetti pericolosi rilevati

Gli oggetti pericolosi rilevati da Kaspersky Internet Security vengono processati con l'uso del pulsante **Disinfetta** (per l'oggetto o gruppo di oggetti selezionati) oppure **Disinfetta tutto** (per elaborare tutti gli oggetti dell'elenco). Dopo l'elaborazione di tutti gli oggetti, comparirà una notifica sullo schermo e l'utente dovrà decidere l'azione successiva.

Spuntando **Applica a tutti** nella finestra di notifica l'azione scelta verrà applicata a tutti gli oggetti aventi il medesimo stato selezionato dall'elenco prima di iniziare l'elaborazione.

19.3.3. La scheda *Eventi*

Questa scheda (vedi Figura 95) contiene un elenco completo degli eventi importanti verificatisi durante il funzionamento di un componente, la scansione antivirus e gli aggiornamenti dei database non esclusi da una regola di controllo delle attività (vedi 10.1 pag. 136).

Questi eventi possono essere:

Eventi critici – eventi di importanza fondamentale che segnalano problemi di funzionamento del programma o vulnerabilità del computer. Per esempio, *virus rilevato*, *errore di funzionamento*.

Eventi importanti – eventi da approfondire poiché riflettono situazioni importanti nel funzionamento del programma. Per esempio, *terminato.*

Messaggi informativi – messaggi di riferimento che di solito non contengono informazioni rilevanti. Per esempio, *OK, non elaborato*. Questi eventi sono riportati nel registro eventi solo spuntando la casella **Mostra tutti gli eventi**.

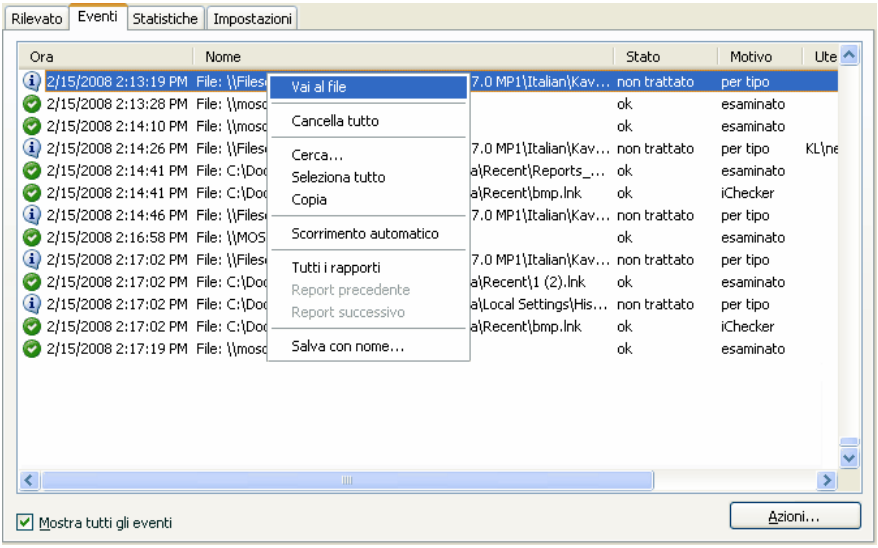


Figura 95. Eventi che si verificano durante il funzionamento di un componente

Il formato di visualizzazione degli eventi nel registro può variare in base al componente o all'attività. Per ogni attività di aggiornamento sono riportate le seguenti informazioni:

- Nome dell'evento.
- Nome dell'oggetto interessato dall'evento.
- L'ora in cui si è verificato l'evento.
- Le dimensioni del file caricato.

Per le attività di scansione antivirus, il registro degli eventi contiene il nome dell'oggetto esaminato e lo stato assegnatogli in seguito alla scansione/elaborazione.

È possibile anche istruire l'Anti-Spam mentre si visualizza il report usando lo speciale menu contestuale. A tal fine, selezionare il nome dell'e-mail ed aprire il menu contestuale cliccando con il tasto destro e selezionare **Segna come Spam**, se l'e-mail è uno spam, oppure **Segna come Non Spam** se l'e-mail selezionata è pulita. Inoltre sulla base delle informazioni ottenute analizzando l'e-

mail è possibile aggiungerla all'elenco bloccati e consentiti di Anti-Spam. A tal fine, usare le voci corrispondenti del menu contestuale.

19.3.4. La scheda *Statistiche*

Questa scheda (vedi Figura 96) contiene le statistiche dettagliate sui componenti e le attività di scansione antivirus. Da questa finestra risulta:

- Quanti oggetti sono stati esaminati in cerca di tratti pericolosi nella sessione corrente di un componente o dopo il completamento di un'attività. Il numero degli archivi, dei file compressi e degli oggetti protetti da password e corrotti esaminati.
- Quanti oggetti pericolosi sono stati rilevati, non disinfettati, eliminati e trasferiti in Quarantena.

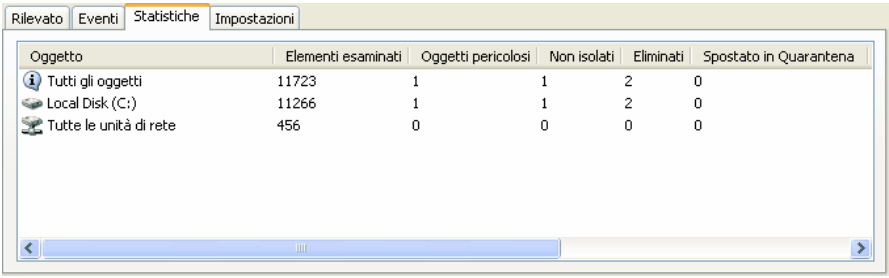


Figura 96. Statistiche del componente

19.3.5. La scheda *Impostazioni*

La scheda **Impostazioni** (vedi Figura 97) visualizza una panoramica completa delle impostazioni dei componenti, delle scansioni antivirus e degli aggiornamenti del programma. È possibile vedere il livello di esecuzione di un componente o di una scansione antivirus, le azioni compiute sugli oggetti pericolosi o le impostazioni in uso per gli aggiornamenti del programma. Usare il link Modifica impostazioni per configurare il componente.

È possibile configurare impostazioni avanzate per le scansioni antivirus:

- Stabilire la priorità delle attività di scansione in caso di sovraccarico sul processore. L'impostazione **Concedi risorse ad altre applicazioni** è selezionata per default. Con questa funzione, il programma individua il carico sul processore e sui sottosistemi del disco per l'attività di altre applicazioni. Se il carico sul processore aumenta considerevolmente e impedisce alle applicazioni dell'utente di funzionare normalmente, il

programma riduce l'attività di scansione. In tal modo si riduce il tempo di scansione e si liberano risorse per le applicazioni dell'utente.

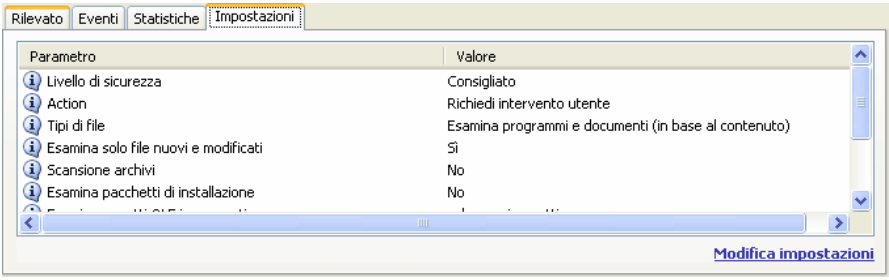


Figura 97. Impostazioni dei componenti

- Impostare la modalità operativa del computer per il periodo successivo al completamento della scansione antivirus. È possibile configurare il computer in modo da spegnersi, riavviarsi o funzionare in standby o in modalità di risparmio. Per selezionare un'opzione, fare clic con il pulsante sinistro del mouse sull'hyperlink fino a visualizzare l'opzione desiderata.

  Questa funzione può risultare utile se, per esempio, si avvia una scansione antivirus al termine della giornata lavorativa e non si desidera aspettarne la conclusione.

  Tuttavia, per poter utilizzare questa funzione è necessario eseguire i seguenti passaggi supplementari: prima di lanciare la scansione è necessario disabilitare le richieste di password per gli oggetti esaminati, se abilitata, e abilitare l'elaborazione automatica degli oggetti pericolosi per disabilitare le funzioni interattive del programma.

19.3.6. La scheda *Registro*

Il programma registra nella scheda **Registro** le operazioni tentate sulle chiavi di registro dall'avvio del programma (vedi Figura 98) , a meno che non vengano inibite da una regola (vedi 10.3.2 pag. 147).

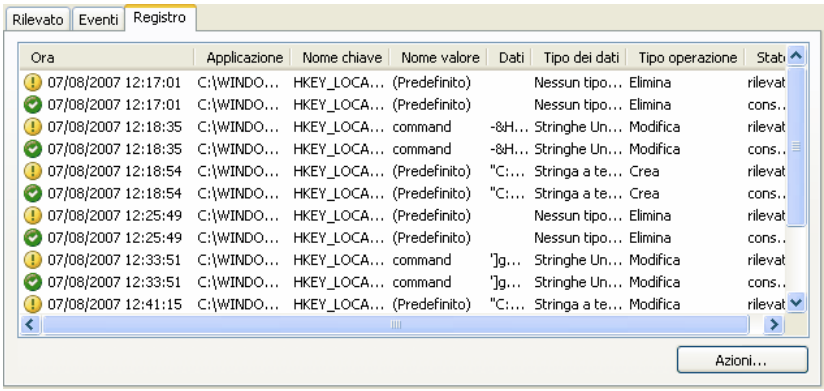


Figura 98. Lettura e modifica degli eventi del registro di sistema

La scheda riporta il nome completo della chiave, il suo valore, il tipo di dati e le informazioni relative all'operazione che ha avuto luogo: l'azione tentata, l'ora e l'eventuale autorizzazione.

19.3.7. La scheda *Tentativi di trasmissione dati*

La scheda report Controllo Privacy mostra tutti i tentativi di ottenere l'accesso ai dati riservati dell'utente ed i tentativi di trasmetterli. Il report indica quale modulo del programma ha tentato di trasmettere i dati, quale evento è stato registrato e l'azione che ha intrapreso il programma.

Per eliminare le informazioni riportate nel report cliccare su **Azioni → Cancella tutto**.

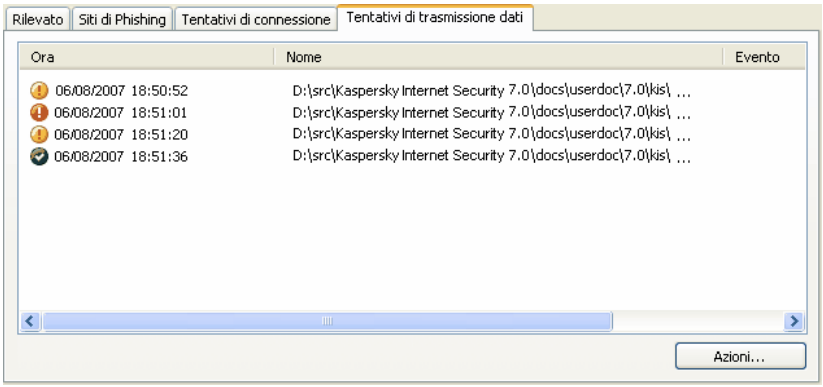


Figura 99. Controllo Privacy

19.3.8. La scheda *Siti di Phishing*

Questa scheda report (vedi Figura 100) mostra tutti i tentativi di phishing trovati durante la corrente sessione di Kaspersky Internet Security. Il report elenca un link al sito phishing riconosciuto nella e-mail (o altra origine), la data e l'ora dell'attacco e lo stato dell'attacco (se è stato bloccato).

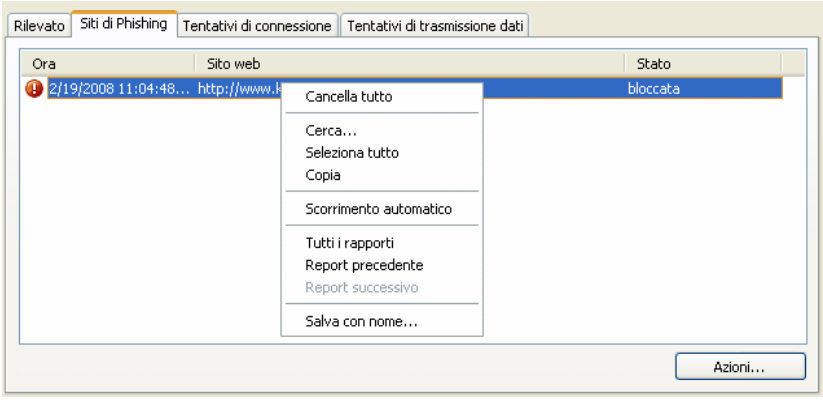


Figura 100. Attacchi phishing bloccati

19.3.9. La scheda *Tentativi di connessione*

Questa scheda (vedi Figura 101) riporta tutti i tentativi computi all'insaputa dell'utente di connessione a siti a pagamento. Questi tentativi sono generalmente condotti da programmi maligni residenti nel computer dell'utente.

Nel report è riportato quale programma ha tentato di comporre il numero telefonico per connettersi ad Internet e se il tentativo è stato bloccato o permesso.

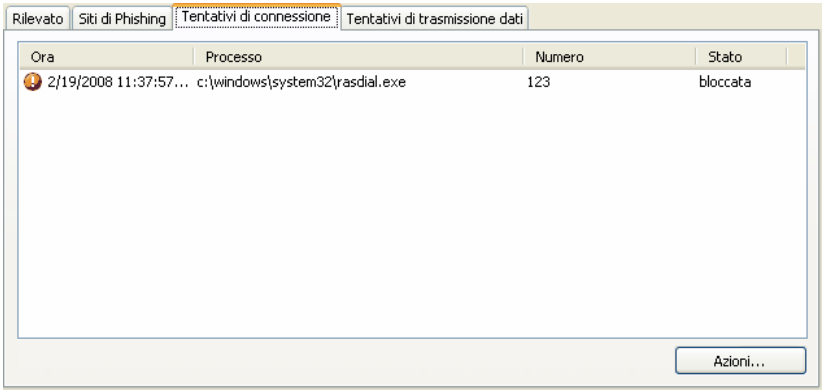


Figura 101. Elenco tentativi connessioni telefoniche

19.3.10. La scheda Attacchi provenienti dalla rete

Questa scheda (vedi Figura 102) mostra una breve sintesi degli attacchi di rete sul computer dell'utente. L'informazione viene registrarla se è abilitato il Sistema di rilevamento delle intrusioni che monitora tutti i tentativi di attacco al computer.

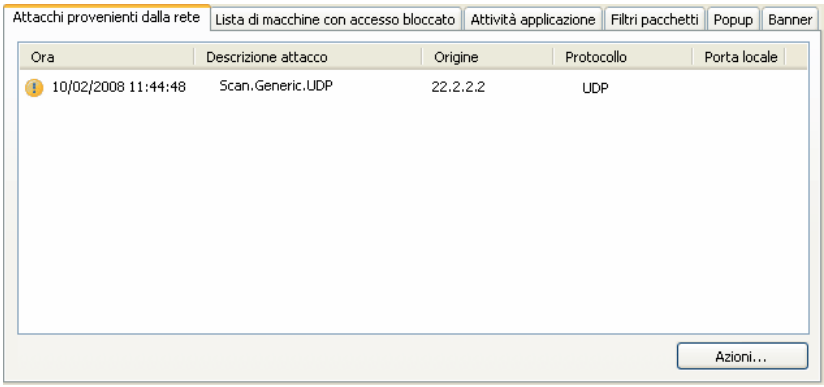


Figura 102. Elenco degli attacchi di rete bloccati

La scheda **Attacchi provenienti dalla rete** elenca le seguenti informazioni sull'attacco:

- Origine dell'attacco. Potrebbe essere un indirizzo IP, un altro computer ecc.
- Porta locale sulla quale è avvenuto il tentativo.
- Breve descrizione dell'attacco.
- L'ora in cui è avvenuto il tentativo.

19.3.11. La scheda *Lista di macchine con accesso bloccato*

Tutti gli host che sono stati bloccati dopo un attacco dal Sistema di rilevamento delle intrusioni vengono elencati in questo report (vedi Figura 103).

Sono riportati il nome ci ciascun host e l'ora in cui sono stati bloccati. È possibile sbloccare un host selezionandolo dall'elenco e cliccando sul pulsante **Azioni** → **Sblocca**.

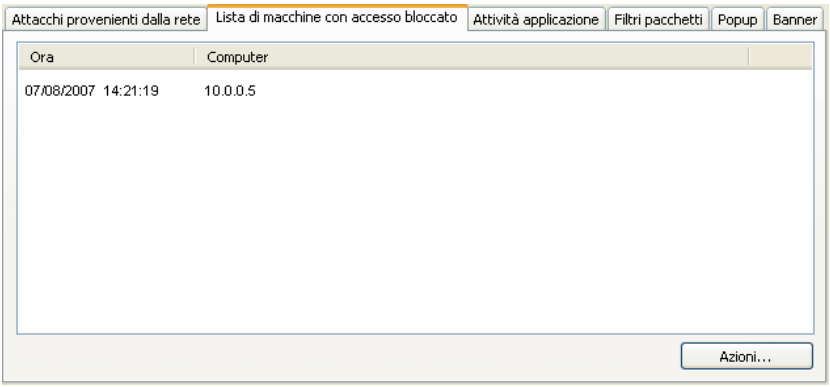


Figura 103. Elenco host bloccati.

19.3.12. La scheda *Attività applicazione*

Nella scheda **Attività applicazione** vengono elencate tutte le applicazioni a cui sono applicate le regole del programma e che sono state registrate dal Sistema di Filtro nel corso dell'attività del Firewall (vedi Figura 104).

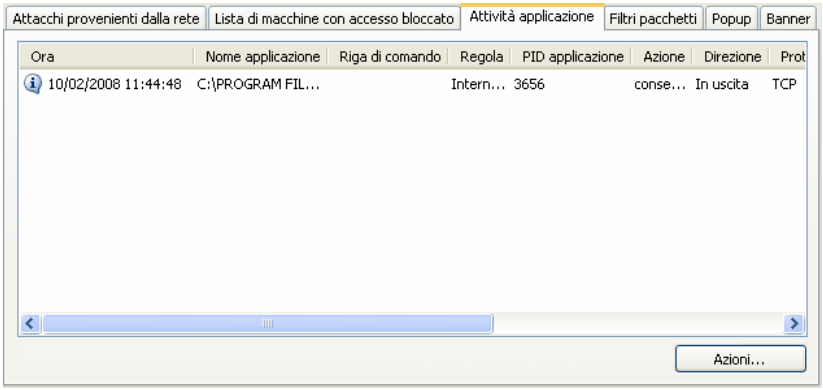


Figura 104. Attività applicazioni monitorate

L'attività viene registrata soltanto se nella regola è selezionata l'opzione **Registra evento**. Per impostazione predefinita, essa è deselezionato nelle regole comprese in Kaspersky Internet Security.

Questa scheda riporta le proprietà di base di ciascuna applicazione (nome, PID, nome della regola) ed un breve sommario della sua attività (protocollo, direzione

del pacchetto ecc). L'informazione è comunque elencata se l'attività dell'applicazione è bloccata.

19.3.13. La scheda *Filtri pacchetti*

La scheda **Filtri pacchetti** contiene le informazioni circa l'invio e la ricezione del pacchetti che incontrano le regole di filtrazione e sono state registrate durante la corrente sessione del Firewall (vedi Figura 105).

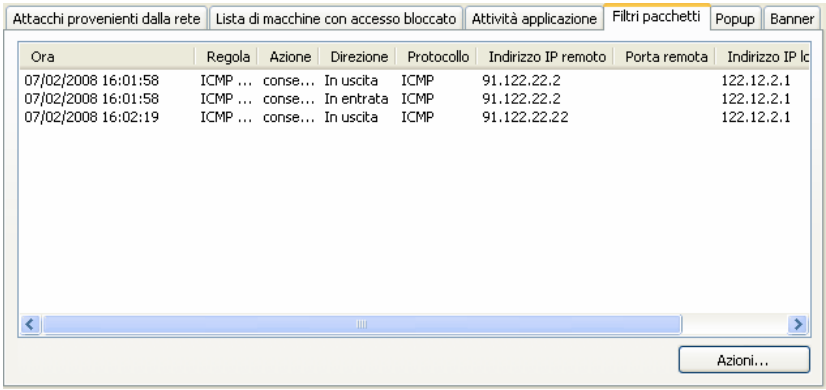


Figura 105. Pacchetti dati monitorati

L'attività viene registrata soltanto se nella regola è selezionata l'opzione **Registra evento**. Per impostazione predefinita, essa è deselezionato nelle regole comprese in Kaspersky Internet Security.

Per ciascun pacchetto sono mostrate (se il pacchetto è stato bloccato) la direzione del pacchetto, il protocollo ed altre impostazioni della connessione di rete per l'invio o la ricezione del pacchetto stesso.

19.3.14. Scheda *Popup*

Questa scheda di report mostra gli URL di tutti i popup bloccati dall'Anti-Pubblicità (vedi Figura 106). Queste finestre generalmente si aprono nei siti web di Internet.

Per ciascun popup vengono registrati l'indirizzo URL, il giorno e l'ora in cui sono stati bloccati.

Figura 106. Elenco dei popup bloccati

19.3.15. Scheda *Banner*

Questa scheda di report del Firewall (vedi Figura 107) elenca gli URL dei banner bloccati dall'*Anti-Banner*. Ciascun banner viene descritto dal suo URL e stato della sua zona: permesso o bloccato.

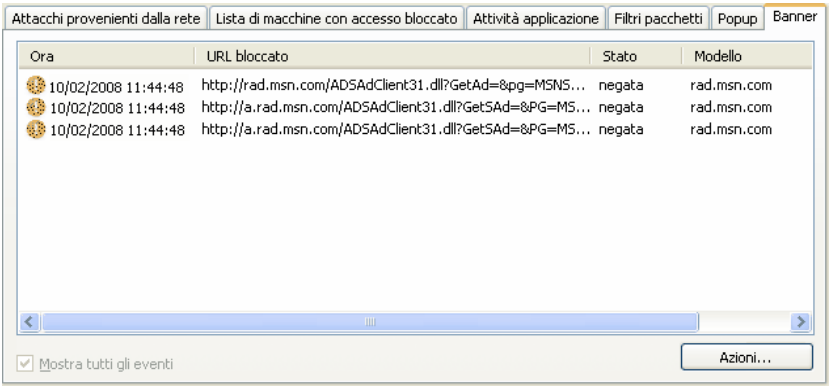


Figura 107. Elenco dei banner bloccati

Ogni banner bloccato può venir riattivato selezionandolo nell'elenco mostrato e cliccando **Azioni** → **Permetti**.

19.3.16. La scheda *Connessioni stabilite*

Tutte le connessioni attive presenti sul computer al momento sono elencate nella scheda **Connessioni stabilite** (vedi Figura 108). Qui sono elencati il nome dell'applicazione che ha avviato la connessione, il protocollo usato, la direzione della connessione (ingresso o uscita) e le impostazioni della connessione (porte locali e remote ed indirizzi IP). Si può anche vedere per quanto tempo una connessione è rimasta attiva ed il volume dei dati ricevuti e trasferiti. È possibile creare o eliminare le regole di connessione. A tal fine, usare la corrispondente opzione nel menu contestuale.

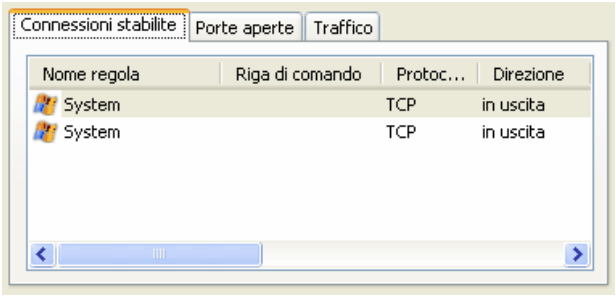


Figura 108. Elenco delle connessioni stabilite

19.3.17. Scheda *Porte aperte*

La scheda **Porte Aperte** elenca tutte le porte al momento aperte per le connessioni di rete (vedi Figura 109). Essa mostra il numero della porta, il protocollo di trasferimento dei dati, il nome dell'applicazione che usa la porta ed il tempo di apertura di ciascuna porta.

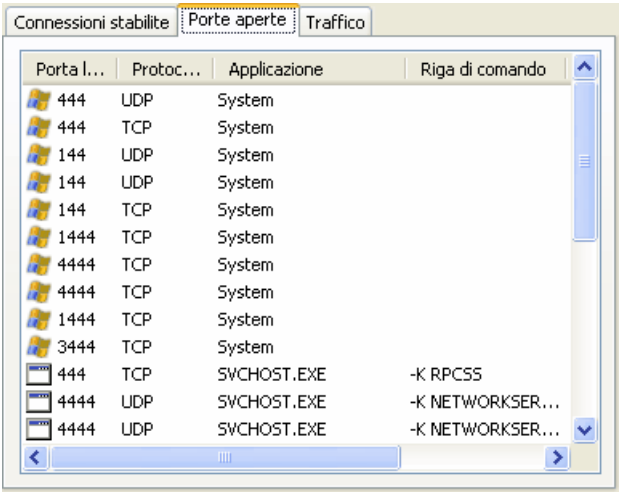


Figura 109. Elenco delle porte aperte sul computerr

Durante l'epidemia di virus e gli attacchi di rete può essere utile conoscere esattamente quale porta risulta vulnerabile. Si può verificare se quella porta è aperta ed esegue i necessari passaggi per proteggere il computer (ad esempio abilitando il Sistema di rilevamento delle intrusioni, chiudendo la porta vulnerabile o creando una regola per essa).

19.3.18. La scheda *Traffico*

Questa scheda (vedi Figura 110) riporta le informazioni circa tutte le connessioni in ingresso ed in uscita tra il computer dell'utente e gli altri computer, compresi web server, server di posta, ecc. L'informazione che segue è data per ciascuna connessione: nome e indirizzo IP dell'host con cui si è connessi e la quantità di traffico inviato e ricevuto.

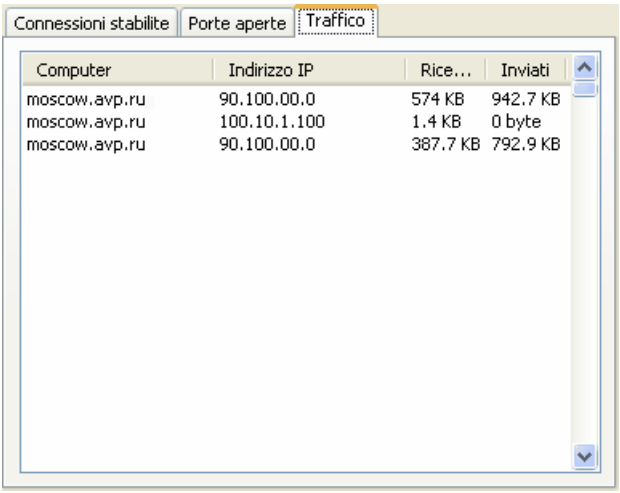


Figura 110. Traffico sulle connessioni di rete stabilite.

19.4. Disco di emergenza

Kaspersky Internet Security dispone di uno strumento per creare un disco di emergenza.

Il disco di emergenza è progettato per consentire il ripristino della funzionalità del sistema dopo un attacco virale che ha danneggiato i file di sistema rendendo impossibile l'avvio del sistema operativo. Il disco include:

- File di sistema di Microsoft Windows XP Service Pack 2.
- Una serie di utility diagnostiche per il sistema operativo.
- I file del programma Kaspersky Internet Security.
- I file contenenti i database.

Per creare un disco di emergenza:

1. Aprire la finestra principale del programma e selezionare **Scansione**.
2. Fare clic su Crea disco di emergenza per procedere alla creazione del disco di emergenza.

Il disco di emergenza viene creato per il computer sul quale è stato creato. L'utilizzo del disco su altri computer può determinare conseguenze imprevedibili, poiché contiene informazioni sui parametri relativi ad un computer specifico (le informazioni sui settori di avvio, ad esempio).

La creazione di un disco di emergenza è possibile solo con sistema operativo Microsoft Windows XP o Microsoft Windows Vista. Non è possibile creare dischi di emergenza sui computer che con sistema operativo Microsoft Windows XP Professional x64 Edition e Microsoft Windows Vista x64.

19.4.1. Creazione di un disco di emergenza

Attenzione!

Per creare un disco di emergenza è necessario disporre del disco di installazione di Microsoft Windows XP Service Pack 2.

Per creare il Disco di emergenza è necessario il programma **PE Builder**.

Prima di creare un disco di emergenza è necessario installare PE Builder sul computer.

Un'apposita procedura guidata guiderà l'utente nella creazione del disco di emergenza. Consiste in una serie di finestre/passaggi fra i quali navigare servendosi dei pulsanti **Indietro** e **Avanti**. Per completare la procedura guidata fare clic su **Fine**. Il pulsante **Annulla** serve per interrompere in qualsiasi momento la procedura.

Passaggio 1. La scrittura del disco

Per creare un disco di emergenza indicare i percorsi alle seguenti cartelle:

- Cartella del programma PE Builder.
- Cartella in cui sono stati salvati i file del disco di emergenza prima di masterizzare il CD/DVD.

  Se non è la prima volta che si crea un disco di emergenza, questa cartella contiene già una serie di file creati la volta precedente. Per usare i file salvati in precedenza, selezionare la casella corrispondente.

Osservare che i file del disco di emergenza creati precedentemente contengono i vecchi database dell'applicazione. Per ottimizzare la scansione antivirus e ripristinare il sistema, si raccomanda di aggiornare i database e di creare un nuovo disco di emergenza.

- Il CD di installazione di Microsoft Windows XP Service Pack 2.

Dopo aver indicato i percorsi alle cartelle richieste, fare clic su **Avanti**. PE Builder si avvia e ha inizio il processo di creazione del disco di emergenza. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

Passaggio 2. Creazione di un file .iso

Dopo che PE Builder ha completato la creazione dei file del disco di emergenza, si apre la finestra **Crea file .iso**.

Il file .iso è un'immagine su CD del disco di emergenza salvata come archivio. La maggior parte dei programmi di masterizzazione CD è in grado di riconoscere correttamente i file .iso (Nero, per esempio).

Se non è la prima volta che si crea un disco di emergenza, è possibile selezionare il file .iso dal disco precedente selezionando **File .iso esistente**.

Passaggio 3. Masterizzazione del disco

Durante la procedura guidata viene chiesto di scegliere se masterizzare il disco di emergenza su CD: adesso o più tardi.

Se si decide di masterizzare immediatamente il disco, specificare se si desidera formattare il disco prima di procedere, selezionando la casella corrispondente. Questa opzione è disponibile solo se si usano dischi CD-RW.

Per avviare la masterizzazione del CD fare clic sul pulsante **Avanti**. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

Passaggio 4. Completamento del disco di emergenza

Questa finestra della procedura guidata informa che il disco di emergenza è stato creato correttamente.

19.4.2. Uso del disco di emergenza

Osservare che Kaspersky Internet Security funziona in modalità provvisoria solo se la finestra principale è aperta. Chiudendo la finestra principale si chiude anche il programma.

Bart PE, il programma predefinito, non supporta i file .chm o i browser di Internet, pertanto in modalità provvisoria non è possibile visualizzare la Guida di Kaspersky Internet Security o i link dell'interfaccia del programma.

Se in seguito a un attacco di virus è impossibile caricare il sistema operativo, procedere come segue:

1. Creare un disco di emergenza utilizzando Kaspersky Internet Security su un computer non infetto.
2. Inserire il disco di emergenza nell'unità CD del computer infetto e riavviare. Microsoft Windows XP SP2 si avvia con l'interfaccia di Bart PE. Bart PE è dotato di assistenza di rete incorporata per usare la propria LAN. All'avvio del programma, viene richiesto se si desidera abilitarlo. Se non è necessario aggiornare i file, disabilitare il supporto di rete.
3. Per aprire Kaspersky Internet Security, fare clic su **Start→Programmi→ Kaspersky Internet Security 7.0 →Start**.

   Si apre la finestra principale di Kaspersky Internet Security. In modalità provvisoria è possibile accedere solo alle scansioni antivirus e agli aggiornamenti dei database dell'applicazione dalla LAN (se era stato abilitato il supporto di rete in Bart PE).
4. Avviare la scansione antivirus.

Notare che i database dell'applicazione vengono usati come default dalla data in cui è stato creato il disco di emergenza. Per questa ragione raccomandiamo di aggiornare i database prima di avviare la scansione.

Occorre anche notare che l'applicazione userà soltanto i database aggiornati con il disco di emergenza durante la corrente sessione, prima di riavviare il computer.

Attenzione!

Se sono stati individuati oggetti infetti o potenzialmente infetti e questi sono stati elaborati e posti in Quarantena o nella cartella Backup allora consigliamo di completare, durante la sessione corrente, il controllo di questi oggetti con un disco di emergenza.

In caso contrario, questi oggetti andranno perduti al riavvio del computer.

19.5. Creazione di un elenco delle porte monitorate

Durante l'uso di componenti come Mail Anti-Virus, Web Anti-Virus, Controllo Privacy ed Anti-Spam vengono monitorati i flussi di dati trasmessi mediante protocolli specifici attraverso determinate porte aperte del computer. Così, per esempio, Mail Anti-Virus analizza le informazioni trasmesse per mezzo del protocollo SMTP mentre Web Anti-Virus analizza quelle trasmesse mediante HTTP.

Il pacchetto del programma include un elenco delle porte più utilizzate per la trasmissione della posta e del traffico HTTP. È possibile aggiungere una nuova porta o disabilitare il monitoraggio di una esistente disabilitando in tal modo il rilevamento di oggetti pericolosi del traffico che passa attraverso la porta in questione.

Per modificare l'elenco delle porte monitorate procedere come segue:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Monitoraggio Traffico**.
2. Cliccare su **Impostazioni Porta**.
3. Aggiorna l'elenco delle porte monitorate nella casella di dialogo **Porte monitorate** (vedi Figura 111).

Figura 111. Elenco delle porte monitorate

Questa finestra presenta un elenco di porte monitorate da Kaspersky Internet Security. Per scansionare il flusso di dati, posizionarsi su tutte le porte aperte del network, selezionare l'opzione **Controlla tutte le porte.** Per modificare manualmente l'elenco delle porte monitorate selezionare **Controlla solo le porte selezionate**.

Per aggiungere una nuova porta all'elenco delle porte monitorate:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Impostazioni porta**.
2. Digitare il numero della porta e una descrizione della stessa negli appositi campi della finestra **Nuova porta**.

Per esempio, il computer possiede una porta non standard attraverso la quale vengono scambiati dati con un computer remoto per mezzo del protocollo HTTP. Web Anti-Virus monitora il traffico HTTP. Per analizzare questo traffico in cerca di codici nocivi, è possibile aggiungere la porta a un elenco di porte controllate.

All'avvio di uno qualsiasi dei suoi componenti, Kaspersky Internet Security apre la porta 1110 come porta di ascolto per tutte le connessioni in entrata. Se in quel momento la porta è occupata, seleziona le porte 1111, 1112, ecc.

Se si usano contemporaneamente Kaspersky Internet Security ed un firewall di un'altra società occorre configurare il firewall per permettere l'accesso del

processo *avp.exe* (il processo interno di Kaspersky Internet Security) a tutte le porte elencate sopra.

Per esempio diciamo che il firewall dell'utente contiene una regola per *iexplorer.ex* che consente a quel processo di stabilire una connessione sulla porta 80.

Quando Kaspersky Internet Security intercetta la query di connessione avviata da *iexplorer.ex* sulla porta 80, la trasferisce su avp.exe che a rotazione tenta di stabilire una connessione con la pagina web in maniera indipendente. Se non esiste una regola di permesso per *avp.exe* il firewall bloccherà quella query. L'utente non potrà avere accesso alla pagina web.

19.6. Scansione delle connessioni protette

Le connessioni effettuate con il protocollo SSL proteggono lo scambio di dati tramite Internet. Il protocollo SSL è in grado di identificare le parti che si scambiano dati tramite certificati elettronici, crittografare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi nocivi, poiché quasi tutti i programmi antivirus non esaminano il traffico SSL.

Kaspersky Internet Security 7.0 offre l'opzione di esaminare il traffico SSL alla ricerca di virus. In caso di tentativo di connessione protetta ad una risorsa Web, verrà visualizzata una notifica sullo schermo (vedi Figura 112) che richiede un intervento dell'utente.

Essa contiene informazioni sul programma che ha avviato la connessione protetta, unitamente all'indirizzo remoto ed alla porta remota. Il programma chiede di decidere se la connessione debba essere esaminata alla ricerca di virus:

- **Elabora** – esamina il traffico alla ricerca di virus in caso di connessione sicura ad un sito Web.

  Si consiglia di esaminare sempre il traffico SSL se ci si sta collegando ad sito Web sospetto o se inizia un trasferimento di dati SSL quando si passa alla pagina successiva. È assai probabile che ciò segnali il trasferimento di un programma nocivo sul protocollo protetto.

- **Evita** – continua la connessione protetta senza esaminare il traffico alla ricerca di virus.

Per applicare l'azione selezionata a tutti i futuri tentativi di stabilire una connessione SSL, selezionare **Applica a tutti**.

Figura 112. Notifica su rilevamento di una connessione SSL

Per esaminare le connessioni crittografate, Kaspersky Internet Security sostituisce il certificato di sicurezza richiesto con un certificato firmato dall'applicazione stessa. In alcuni casi, i programmi che stabiliscono la connessione non accetteranno questo certificato e la connessione non può essere stabilita. Si consiglia di selezionare l'opzione **Evita** nella notifica relativamente alla scansione delle connessioni protette:

- Durante il collegamento ad una risorsa Web attendibile, ad esempio la pagina Web della propria banca, dalla quale gestire il proprio conto corrente. In questo caso, è importante che l'autenticità del certificato della banca venga confermata.
- Se il programma che stabilisce la connessione verifica il certificato del sito web al quale si accede. Ad esempio, MSN Messenger verifica l'autenticità della firma digitale di Microsoft Corporation quando stabilisce una connessione al server.

È possibile configurare le impostazioni della scansione SSL dalla scheda **Monitoraggio del traffico** nella finestra delle impostazioni dell'applicazione (vedi Figura 113).

Controlla tutte le connessioni crittografate – esamina tutto il traffico in entrata tramite protocollo SSL alla ricerca di virus.

Richiesta di scansione al rilevamento di una nuova connessione criptata – visualizza un messaggio che richiede l'intervento dell'utente ogniqualvolta viene stabilita una connessione SSL.

Non controllare connessioni crittografate – non esamina il traffico in entrata tramite protocollo SSL alla ricerca di virus.

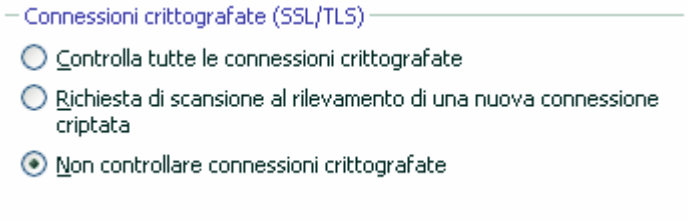


Figura 113. Configurazione della scansione delle connessioni protette

19.7. Configurazione del Server Proxy

La connessione ad un server proxy può essere configurata usando la sezione Server Proxy (vedi Figura 114) nella finestra impostazioni dell'applicazione (se la connessione a Internet avviene attraverso un proxy). Kaspersky Internet Security utilizza questa impostazioni per molti moduli di protezione in tempo reale e per aggiornare i database ed i moduli dell'applicazione

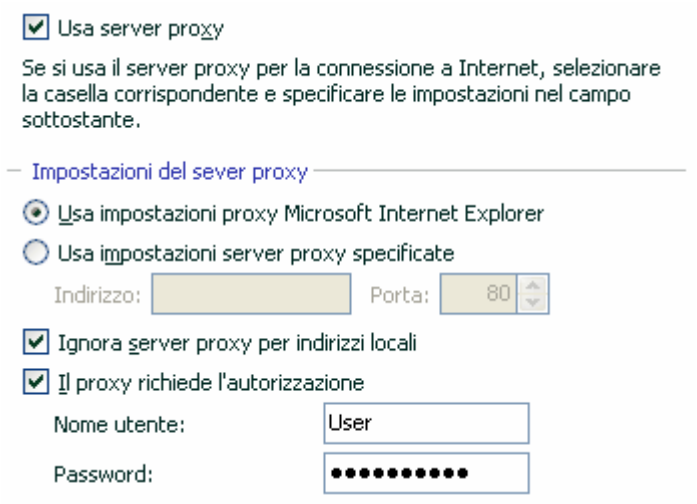


Figura 114. Configurazione di Server Proxy

Se si usa un server proxy per connettersi ad Internet spuntare **Usa Server Proxy** e configurare le seguenti impostazioni secondo necessità:

- Selezionare i parametri del server proxy da usare:

  Usa impostazioni proxy per Microsoft Internet Explorer. Se questa opzione è selezionata le impostazioni del server proxy sono riconosciute automaticamente usando il protocollo WPAD (Web Proxy Auto-Discovery Protocol). Se il protocollo non riesce a determinare l'indirizzo, Kaspersky Internet Security usa le impostazioni specificate per Microsoft Internet Explorer.

  Usa impostazioni server proxy specificate: usa un server proxy diverso da quello specificato nelle impostazioni della connessione al browser. Digitare un indirizzo IP o il nome di un dominio nel campo **Indirizzo** e il numero della porta del server proxy nel campo **Porta**.

  Per non usare un server proxy per gli aggiornamenti da directory locali o di rete, spuntare **Ignora server proxy per indirizzi locali.**

- Specificare se il server proxy utilizza l'autenticazione. L'Autenticazione è una procedura per verificare le informazioni dell'utente allo scopo di controllarne l'accesso.

  Se è richiesta l'autenticazione per connettersi al server proxy spuntare **Il proxy richiede l'autorizzazione** ed inserire nome utente e

password nei campi appropriati. Verrà eseguita una autorizzazione NTLM seguita da una autorizzazione BASIC.

Se la casella non è spuntata l'autorizzazione NTLM verrà condotta usando il login con cui viene avviata l'azione (come per un aggiornamento, vedi 6.6 pag. 78).

Se il server proxy richiede una autorizzazione ma il nome utente e la password non sono indicati o rifiutati dal proxy per qualsiasi ragione, comparirà una finestra di dialogo che richiederà nome utente e password. Se l'autorizzazione ha esito positivo lo specifico nome utente e password verranno ricordati per un uso successivo. Altrimenti verrà nuovamente richiesta l'autorizzazione.

Premendo il pulsante **Annulla** nella finestra di dialogo di richiesta dell'autenticazione, si sostituisce l'origine corrente degli aggiornamenti con quella successiva in elenco; i parametri di autenticazione specificati in quella finestra o definiti nell'interfaccia del programma saranno ignorati. Pertanto, l'applicazione tenterà un'autenticazione NTLM in base all'account usato per lanciare l'attività.

Se si usa un server ftp per gli aggiornamenti viene eseguita una connessione passiva al server. Se questa connessione dà errore, si tenta di stabilire una connessione attiva.

Per impostazione predefinita, il tempo di connessione al server degli aggiornamenti è di 1 minuto. Se la connessione cade si tenterà la connessione ad un altro server di aggiornamento al termine del periodo. Questo si ripete fino a che l'operazione ha successo oppure fino a che tutti i server degli aggiornamenti sono stati contattati.

19.8. Configurazione dell'interfaccia di Kaspersky Internet Security

Kaspersky Internet Security offre la possibilità di modificare l'aspetto del programma creando e utilizzando nuovi stili. È possibile inoltre configurare l'uso degli elementi attivi dell'interfaccia come l'icona nell'area di notifica della barra delle applicazioni e i popup.

Per configurare l'interfaccia del programma procedere come segue:

Aprire la finestra impostazioni dell'applicazione e seleziona **Aspetto** (vedi Figura 115).

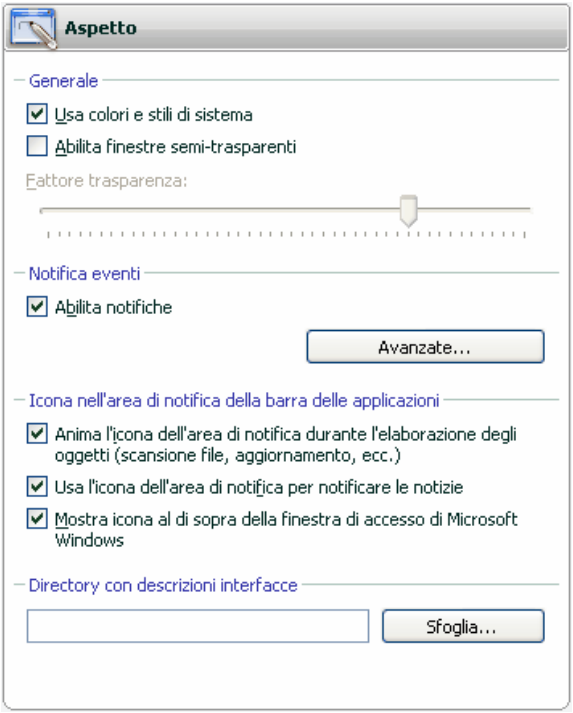


Figura 115. Configurazione delle impostazioni dell'interfaccia del programma

Nella parte destra della finestra delle impostazioni, è possibile configurare:

- *Componenti grafici e colori definiti dall'utente per l'interfaccia dell'applicazione*

  Per impostazione predefinita, l'interfaccia grafica usa un insieme di colori e stili. Questi possono essere modificati spuntando **Usa colori e stili di sistema**. Questo abilita gli stili specificati nella configurazione dei temi del display.

  Tutti i colori, le font, le icone ed i testi usati nell'Interfaccia di Kaspersky Internet Security sono configurabili. Possono essere anche creati skin personalizzati per l'applicazione. L'applicazione stessa può essere localizzata in un'altra lingua. Per inserire una skin, immettere la directory contenente la sua descrizione in **Directory con descrizioni interfacce**. Usare il pulsante **Sfoglia** per selezionare una directory

- *Grado di trasparenza dei messaggi pop-up*

  Tutte le operazioni di Kaspersky Internet Security che richiedono la notifica all'utente o il suo intervento immediato sono comunicate in un messaggio pop-up sopra l'icona dell'applicazione nell'are di notifica della barra delle applicazioni. Le finestre del messaggio sono trasparenti in modo da non interferire con il lavoro. Se si muove il cursore sul messaggio, la trasparenza svanisce. Il grado di trasparenza di questi messaggi può essere modificato regolando la scala del **Fattore trasparenza** sulla posizione desiderata. Per eliminare la trasparenza del messaggio, deselezionare la casella **Abilita finestre semi-trasparenti**.

- *Animazione dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni*

  A seconda dell'operazione eseguita dal programma, l'icona nell'area di notifica cambia. Per esempio, durante la scansione di uno script compare sullo sfondo dell'icona una piccola rappresentazione, mentre durante la scansione di un messaggio e-mail compare una busta. L'animazione delle icone è abilitata per impostazione predefinita. Se si desidera disabilitare l'animazione, deselezionare la casella **Anima l'icona dell'area di notifica durante l'elaborazione degli oggetti**. Da quel momento in poi l'icona rappresenta solo lo stato di protezione del computer: se la protezione è abilitata l'icona è a colori, mentre se la protezione è in pausa o disabilitata l'icona diventa grigia.

- *Notifica delle notizie da parte di Kaspersky Lab*

  Per impostazione predefinita, se l'utente riceve delle news compare un'icona speciale nell'area di notifica che, quando spuntata, mostra il contenuto della notizia. Per disabilitare la notifica deselezionare **Usa l'icona dell'area di notifica per notificare le notizie**.

- *Visualizzazione dell'icona di Kaspersky Internet Security all'avvio del sistema operativo*

  Per impostazione predefinita, questo indicatore appare nell'angolo superiore destro dello schermo quando si carica il programma. Esso informa l'utente che il computer è protetto da tutti i tipi di minaccia. Per non visualizzare questo indicatore, deselezionare **Mostra icona al di sopra della finestra di accesso di Microsoft Windows**.

Osservare che le impostazioni dell'interfaccia di Kaspersky Internet Security definite dall'utente non vengono salvate in caso di ripristino delle impostazioni predefinite o di disinstallazione del programma.

19.9. Uso delle opzioni avanzate

Kaspersky Internet Security offre le seguenti funzioni avanzate (vedi Figura 116):

- avvio di Kaspersky Internet Security all'avvio del sistema operativo (vedi 19.11 pag. 310);
- notifica all'utente di certi eventi dell'applicazione (vedi 19.9.1 pag. 301);
- Auto-Difesa di Kaspersky Internet Security da chiusura, rimozione o modifica dei moduli e da protezione tramite password dell'applicazione (vedi 19.9.2 pag. 305);
- esportazione/importazione delle impostazioni di funzionamento di Kaspersky Internet Security (vedi 19.9.3 pag. 307);
- ripristino delle impostazioni predefinite (vedi 19.9.4 pag. 307).

Per configurare queste funzioni:

Aprire la finestra impostazioni dell'applicazione e selezionare **Servizio**.

Nella parte destra dello schermo è possibile specificare se abilitare le funzioni avanzate durante l'uso del programma.

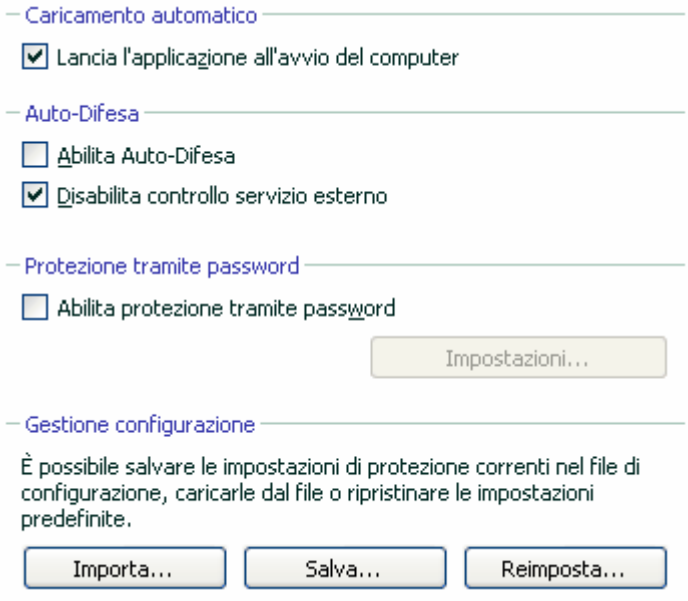


Figura 116. Configurazione delle opzioni avanzate

19.9.1. Notifiche degli eventi di Kaspersky Internet Security

Durante l'uso di Kaspersky Internet Security si verificano diversi tipi di eventi. Le notifiche corrispondenti possono essere informative o contenere dati importanti. Per esempio, un messaggio può informare dell'avvenuto aggiornamento del programma oppure registrare l'errore di un componente che deve essere risolto immediatamente.

Per ricevere gli aggiornamenti sul funzionamento di Kaspersky Internet Security è possibile utilizzare la funzione di notifica.

Le notifiche possono essere trasmesse in vari modi:

- In forma di messaggi pop-up sopra l'icona del programma nell'area di notifica della barra di sistema
- Con segnali acustici
- Con e-mail
- Con un registro eventi

Per usare questa funzione procedere come segue:

1. Selezionare la casella **Abilita notifiche** sotto **Notifica eventi** nella sezione **Aspetto** della finestra delle impostazioni dell'applicazione (vedi Figura 115).
2. Definire i tipi di evento per cui si vuole ricevere la notifica di Kaspersky Internet Security ed il metodo di consegna della stessa (vedi 19.9.1.1 pag. 301).
3. Configurare le impostazioni di consegna della notifica via e-mail, se questo è il metodo di notifica da usare (vedi 19.9.1.2 pag. 303).

19.9.1.1. Tipi di eventi e metodo di consegna della notifica

Durante l'uso di Kaspersky Internet Security, possono verificarsi i seguenti tipi di eventi:

Notifiche critiche sono eventi di importanza cruciale. Si raccomanda di abilitare gli avvisi, poiché questo tipo di eventi segnala la presenza di problemi di funzionamento del programma o di vulnerabilità della protezione del computer. Per esempio, *database dell'applicazione danneggiato* o *licenza scaduta*.

Errori funzionali – sono eventi che impediscono l'attività dell'applicazione. Ad esempio *nessuna chiave o database.*

Notifiche importanti – sono eventi che devono essere investigati poiché riflettono importanti situazioni nell'operatività del programma. Ad esempio *protezione disabilitata o computer non scansionato per molto tempo*.

Notifiche informative. Ad esempio *disinfettati tutti gli oggetti pericolosi*

Per specificare gli eventi da notificare e le modalità di notifica:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Aspetto** (vedi Figura 115).
2. Spunta **Abilita Notifiche** sotto **Notifica Eventi** e andare sulle impostazioni avanzate ciccando su **Avanzate**.

È possibile configurare i seguenti metodi di notifica per gli eventi sopra elencati nella finestra di dialogo **Impostazioni di notifica eventi** (vedi Figura 117):

- *Messaggi pop-up* sopra l'icona del programma nella barra di sistema, contenenti informazioni sull'evento verificatosi.

  Per usare questo tipo di notifica, selezionare la casella nella sezione **Area** in corrispondenza dell'evento del quale si desidera essere informati.

- *Segnale acustico*

  Se si desidera che l'avviso sia accompagnato da un segnale acustico, selezionare la casella **Suono** in corrispondenza dell'evento.

- *Notifica E-mail*

  Per utilizzare questo tipo di notifica, selezionare la casella **E-mail** dell'evento del quale si desidera essere informati, e configurare le impostazioni di invio delle notifiche (vedi 19.9.1.2 pag. 303).

- *Registro eventi*

  Per registrare le informazioni a proposito degli eventi avvenuti spuntare la casella nella colonna **Registro** e configurare le impostazioni del registro eventi (vedi 19.9.1.3 pag. 304).

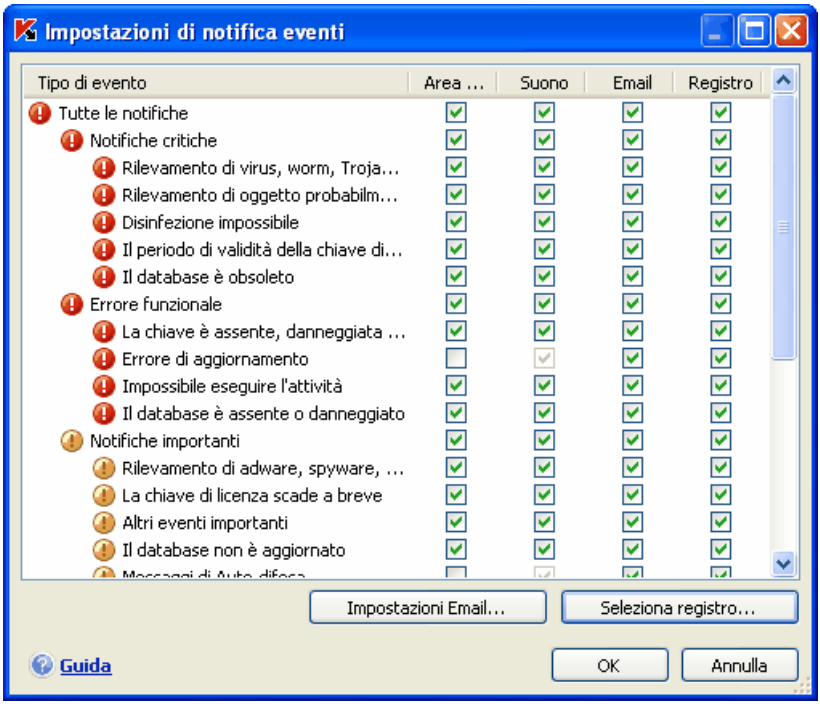


Figura 117. Eventi del programma e metodi di notifica

19.9.1.2. Configurazione delle notifiche via e-mail

Dopo aver selezionato gli eventi (vedi 19.9.1.1 pag. 301) dei quali si desidera essere informati per e-mail, è necessario configurare la consegna dell'avviso procedendo come segue:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Aspetto** (vedi Figura 115).
2. Cliccare su **Avanzate** sotto **Notifica Eventi**.
3. Usare la finestra **Impostazioni di notifica eventi** (vedi Figura 118) per spuntare gli eventi che dovrebbero innescare la notifica e-mail nella colonna **E-mail**.
4. Nella finestra che si apre (vedi Figura 118) cliccando su **Impostazioni E-mail**, configurare le seguenti impostazioni per le notifiche e-mail:
   - Impostare la notifica di invio per **Da - Indirizzo e-mail**:

- Specificare l'indirizzo e-mail a cui inviare gli avvisi in **A indirizzo e-mail**.
- Impostare il metodo di consegna della notifica per e-mail in **Modalità invio**. Se si desidera che il programma invii il messaggio non appena l'evento si verifica, selezionare **Immediatamente quando si verifica l'evento**. Per la notifica di eventi entro un determinato periodo di tempo, impostare il calendario di invio dei messaggi informativi facendo clic su **Cambia**. Gli invii quotidiani sono l'impostazione predefinita.

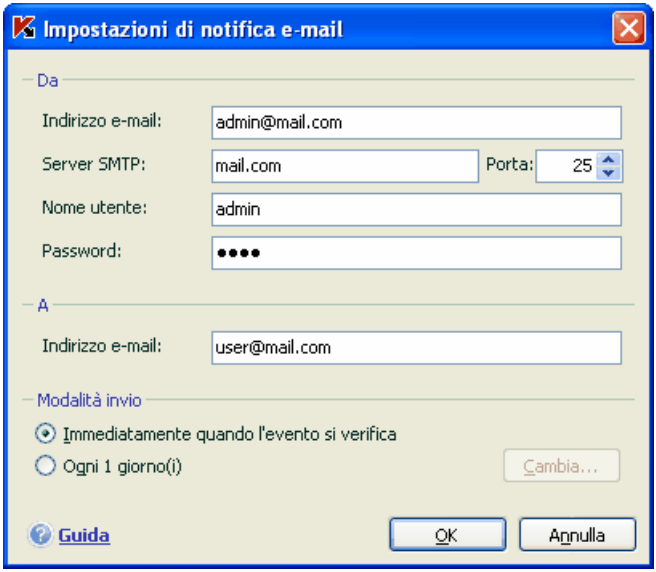


Figura 118. Configurazione impostazioni notifiche e-mail

19.9.1.3. Configurzione delle impostazione del registro eventi

Per configurare le impostazioni del registro eventi:

1. Aprire la finestra impostazioni dell'applicazione e selezionare **Aspetto** (vedi Figura 115).
2. Cliccare su **Avanzate** sotto **Notifica Eventi**.

Usare la finestra **Impostazioni di Notifica Eventi** per selezionare l'opzione di log informativo per un evento e fare clic sul pulsante **Seleziona registro**.

Kaspersky Internet Security ha la possibilità di registrare l'informazione circa l'evento si verifica sorge mentre il programma è in funzione, sia nel registro eventi generale di Microsoft Windows (**Applicazione**) o in uno dedicato da Kaspersky Internet Security (**Registro eventi Kaspersky**).

I registri possono essere visti nel **Visualizzatore Eventi** di Microsoft Windows, apribile attraverso **Start/Pannello di controllo/Strumenti di amministrazione/Visualizzatore eventi**.

19.9.2. Auto-Difesa e limitazioni d'accesso

Kaspersky Internet Security è una applicazione che garantisce la protezione del computer dai programmi nocivi e, proprio per questo, è spesso oggetto di attacchi da parte di programmi nocivi che cercano di bloccarne l'attività o perfino di rimuoverlo dal computer.

Inoltre è possibile che più utenti si servano di un unico computer, non tutti ugualmente esperti nell'uso. Lasciare libero accesso al programma e alle sue impostazioni, pertanto, riduce considerevolmente la sicurezza del computer.

Per garantire la stabilità del sistema operativo, il programma è stato dotato di meccanismi di protezione automatica, protezione dall'accesso remoto e protezione mediante password.

Sui computer dotati di sistema operativo a 64 bit e Microsoft Windows Vista l'autodifesa è disponibile solo per evitare che i file propri del programma sui drive locali e sul registro di sistema siano modificati o eliminati.

Per abilitare Auto-Difesa:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Servizio** (vedi Figura 116).
2. Effettuare le seguenti configurazioni nel riquadro **Auto-Difesa** (Figura 116):

   ☑ **Abilita Auto-Difesa.** Se questa casella è selezionata, il programma protegge i propri file, i processi nella memoria e le voci nel registro di sistema dall'eliminazione o dalla modifica.

   ☑ **Disabilita controllo servizio esterno**. Se questa casella è selezionata, qualsiasi tentativo di uso del programma da parte di amministrazioni remote viene bloccato.

   Affinché i tool di amministrazione remota (come RemoteAdmin) possano accedere a Kaspersky Anti-Virus, questi dovrebbero essere aggiunti all'elenco delle applicazioni attendibili e l'opzione

Non limitare attività applicazione dovrebbe essere abilitata (vedi 6.9.2 a pag. 88).

In presenza di qualsiasi azione tra quelle sopra elencate, viene visualizzato un messaggio sopra l'icona del programma nell'area di notifica di sistema (se il servizio di notifica non è stato disabilitato dall'utente).

Per proteggere il programma mediante password, selezionare la casella **Abilita protezione tramite password** nell'area con lo stesso nome. Cliccare sul pulsante **Impostazioni** per aprire la finestra Protezione tramite password e digitare la password e l'area che la restrizione all'accesso coprirà (vedi Figura 119). È possibile bloccare qualsiasi operazione del programma, ad eccezione della notifica di rilevamento di oggetti pericolosi, o impedire l'esecuzione di qualsiasi tra le seguenti azioni:

- Modifica delle impostazioni del programma.
- Chiusura di Kaspersky Internet Security.
- Disattivazione o sospensione della protezione del computer.

Ciascuna delle azioni sopra elencate riduce la sicurezza del computer ed è quindi necessario stabilire quali tra gli utenti del computer sono sufficientemente attendibili da poter compiere tali azioni.

Selezionando questa opzione, ogni volta che un utente del computer cerca di eseguire le azioni selezionate, il programma richiede una password.

Figura 119. Impostazioni della password di protezione del programma

19.9.3. Importazione ed esportazione delle impostazioni di Kaspersky Internet Security

Kaspersky Internet Security offre la possibilità di importare ed esportare le impostazioni dell'applicazione.

Questa funzione risulta particolarmente utile nei casi in cui, per esempio, il programma è installato sia nel computer di casa sia in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, salvare queste impostazioni su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

Per esportare le impostazioni correnti del programma:

1. Aprire la finestra impostazioni del programma e selezionare la sezione **Servizio** (vedi Figura 116).
2. Cliccare sul pulsante **Salva** nella sezione **Gestione Configurazione**.
3. Digitare un nome per il file di configurazione e selezionare una destinazione in cui salvarlo.

Per importare le impostazioni da un file di configurazione:

1. Aprire la finestra delle impostazioni del programma e selezionare la sezione **Servizio**.
2. Fare clic sul pulsante **Importa** e selezionare il file dal quale importare le impostazioni di Kaspersky Internet Security.

19.9.4. Ripristino delle impostazioni predefinite

È possibile ripristinare le impostazioni predefinite del programma in qualsiasi momento. Esse infatti sono considerate ottimali e consigliate dagli esperti di Kaspersky Lab. A tal fine, servirsi della procedura guidata.

Per ripristinare le impostazioni di protezione:

1. Aprire la finestra delle impostazioni dell'applicazione e selezionare **Servizio** (vedi Figura 116).
2. Cliccare sul pulsante **Reimposta** nella sezione **Gestione configurazione**.

La finestra che si apre chiede all'utente di defnire quali impostazioni ripristinare ai rispettivi valori predefiniti.

La finestra elenca i componenti del programma le cui impostazioni sono state modificate dall'utente, o che il programma ha acquisito con l'apprendimento (di Firewall o Anti-Spam). Verranno mostrate anche le eventuali impostazioni speciali create per i componenti.

Esempi di impostazioni speciali potrebbero essere le frasi e i mittenti degli elenchi Bloccati e Consentiti di Anti-Spam, gli indirizzi attendibili e gli indirizzi bloccati, oltre ai numeri di telefono ISP consentiti e bloccati di Web Anti-Virus e Controllo Privacy; regole di esclusione create per i componenti del programma; regole di applicazione e di filtro pacchetti per il Firewall e regole di applicazione per Difesa Proattiva.

Questi elenchi vengono creati man mano che si utilizza il programma, in base alle attività individuali e ai requisiti di sicurezza. Questo processo di solito richiede tempo, pertanto si consiglia di salvare tali impostazioni prima di ripristinare le impostazioni predefinite del programma.

Il programma salva per impostazione predefinita tutte le impostazioni personalizzate dell'elenco (sono deselezionate). Per non salvare una delle impostazioni, selezionare la casella corrispondente.

Al termine della configurazione delle impostazioni, premere il pulsante **Avanti**. Si apre la procedura guidata (vedi 3.2 pag. 40). Seguire le istruzioni.

Al termine della procedura guidata, per tutti i componenti viene impostato il livello di protezione **Consigliato**, con l'eccezione delle impostazioni che l'utente decide di mantenere. Vengono applicate inoltre le impostazioni configurate con la procedura guidata.

19.10. Supporto Tecnico

Informazioni circa il supporto tecnico reso disponibile da Kaspersky Internet Security sono fornite sotto **Supporto** (vedi Figura 120) nella finestra principale dell'applicazione.

La sezione superiore presenta informazioni generali dell'applicazione, data di pubblicazione del database come pure un riepilogo del sistema operativo del tuo computer.

Se dovesse sorgere un problema durante il funzionamento di Kaspersky Internet Security, per prima cosa verificare che le istruzioni circa l'inconveniente riscontrato siano assenti dalla guida del presente programma o dalla Knowledge Base sul sito web del Supporto Tecnico di Kaspersky Lab. La Knowledge Base è una sezione separata del sito del Supporto Tecnico e comprende consigli per i prodotti di Kaspersky Lab e le risposte alle domande più frequenti. Tentare di

usare questa risorsa per trovare una risposta alla propria domanda o una soluzione ad essa. Cliccare su Assistenza Web per spostarsi sulla Knowledge Base.

Il forum degli utenti di Kaspersky Lab è una altra risorsa per le informazioni sull'applicazione. Esso è in una sezione separata del sito del Supporto Tecnico e contiene le domande degli utenti, risposte e richieste. È possibile vedere gli argomenti fondamentali, lasciare commenti o trovare una risposta ad una propria domanda. Cliccare su Forum Utenti per andare su questa risorsa.

Se non si trova una soluzione al proprio problema nella Guida, nella Knowledge Base o nel Forum per gli utenti, contattare il Supporto Tecnico di Kaspersky Lab.

Notare che occorre essere un utente registrato di una versione commerciale di Kaspersky Internet Security per avere diritto al supporto tecnico. Nessun supporto è fornito per le versioni di prova.

Se l'applicazione è stata attivata con un codice di attivazione, la registrazione dell'utente avviene mediante la procedura guidata di attivazione (vedi 3.2.2 pag. 40). Verrà assegnato un ID cliente ed al termine della registrazione che può essere visualizzato sotto Supporto (vedi Figura 120) nella finestra principale. Il numero cliente è un ID personale che viene richiesto per il supporto telefonico o nella modulistica presente sul sito web.

Se per l'attivazione è stato usato un file chiave, registrarsi direttamente sul sito web del Supporto Tecnico.

Un nuovo servizio detto Assistenza personalizzata fornisce agli utenti l'accesso ad una sezione personale del Supporto Tecnico sul web. L'assistenza personalizzata abilita l'utente a:

- inviare richieste al Supporto Tecnico senza accedere al sito;
- scambiare messaggi con il Supporto Tecnico via e-mail;
- monitorare le richieste in tempo reale;
- vedere la cronologia delle proprie richieste al Supporto Tecnico;
- ottenere una copia di backup del file della chiave.

Usare il link Sottoporre una domanda per inviare con un modulo on-line la tua richiesta al Supporto Tecnico. Entrare nel proprio spazio di assistenza personalizzata sul sito del Supporto Tecnico che si apre e compilare il modulo di richiesta.

Utilizzare il link Corsi on-line per ottenere ulteriori informazioni sugli eventi di training sui prodotti Kaspersky Lab.

Figura 120. Informazioni Supporto Tecnico

Per una assistenza urgente usare il numero telefonico fornito nella Guida del programma (vedi B.2 pag. 349). Il supporto telefonico è sempre attivo (24 ore su 24 ore per 7 giorni la settimana) in Russo, Inglese, Francese, Tedesco e Spagnolo.

19.11. Chiusura dell'applicazione

Per chiudere Kaspersky Internet Security, selezionare **Esci** dal menu contestuale dell'applicazione (vedi 4.2 pag. 53). Ciò causerà lo scarico dell'applicazione della RAM il che significa che il computer non sarà più protetto.

Qualora fossero aperte delle connessioni di rete al momento della chiusura, sarà visualizzato un messaggio che informa che queste connessioni sono state interrotte. Ciò è richiesto affinché l'applicazione si chiuda correttamente. La disconnessione avviene automaticamente dopo 10 secondi oppure facendo clic

su **Sì**. La maggior parte di queste connessioni vengono ristabilite dopo un certo periodo di tempo.

Notare che qualsiasi download in corso durante l'interruzione della connessione viene altrettanto interrotto a meno che non stia usando un download manager. Per recuperare il file occorre riavviare il download.

Per evitare che la connessione venga interrotta, cliccare su **No** nella finestra di notifica. Di conseguenza l'applicazione continuerà a funzionare.

Se l'applicazione viene arrestata, la protezione può essere riabilitata riavviando Kaspersky Internet Security selezionando **Start → Tutti i programmi → Kaspersky Internet Security 7.0 → Kaspersky Internet Security 7.0**.

La protezione ripartirà automaticamente in seguito ad un reboot del sistema operativo. Per abilitare questa modalità seleziona **Servizio** (vedi Figura 116) nella finestra delle impostazioni dell'applicazione e spuntare ☑ **Lancia l'applicazione all'avvio del computer** sotto **Caricamento automatico**.

CAPITOLO 20. USO DEL PROGRAMMA DALLA RIGA DI COMANDO

Kaspersky Internet Security può essere utilizzato anche dalla riga di comando eseguendo le seguenti operazioni:

- Avvio, arresto, pausa e ripristino dell'attività dei componenti dell'applicazione.
- Avvio, arresto, pausa e ripristino delle scansioni antivirus.
- Ottenimento di informazioni sullo stato corrente di componenti, attività e statistiche.
- Scansione di oggetti selezionati.
- Aggiornamento dei database e dei moduli del programma.
- Accesso alla Guida per consultare la sintassi dei prompt di comando.
- Accesso alla Guida per consultare la sintassi dei comandi.

La sintassi della riga di comando è la seguente:

```
avp.com <command> [Impostazioni]
```

Occorre accedere al programma dal prompt di comando dalla cartella di installazione del programma o specificando il percorso completo a avp.com.

Possono essere usati come **<comandi>** i seguenti:

ACTIVAE	Attiva l'applicazione via Internet usando un codice di attivazione
ADDKEY	Attiva l'applicazione usando un file chiave (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
START	Avvia un componente od una azione

PAUSE	Mette in pausa un componente o una azione (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
RESUME	Riavvia un componente o attività
STOP	Termina un componente o attività (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
STATUS	Visualizza lo stato del componente o attività correnti
STATISTICS	Visualizza le statistiche del componente o attività
HELP	Fornisce indicazioni sulla sintassi dei comandi e sull'elenco dei comandi
SCAN	Esegue la scansione antivirus di oggetti
UPDATE	Avvia l'aggiornamento del programma
ROLLBACK	Ritorna all'ultimo aggiornamento eseguito (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
EXIT	Chiude il programma (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
IMPORT	Importa le impostazioni di Kaspersky Internet Security (il comando può essere eseguito solo se viene inserita la password impostata nell'interfaccia del programma)
EXPORT	Esporta le impostazioni di Kaspersky Internet Security

Ogni comando utilizza le impostazioni specifiche del componente corrispondente di Kaspersky Internet Security.

20.1. Attivazione dell'applicazione

Il programma può essere attivato in due modi:

- via Internet usando un codice di attivazione (comando ATTIVAZIONE)
- usando un file con la chiave (comando ADDKEY)

Sintassi di comando:

```
ACTIVATE <codice_attivazione>
ADDKEY >nome_file> /password=<la_tua_password>
```

Descrizione dei parametri:

<codice_attivazione>	Il codice di attivazione del programma fornito con l'acquisto
<nome_file>	Nome del file della chiave con l'estensione *.key*
<la_tua_password>	La password impostata con l'interfaccia di Kaspersky Internet Security
Notare che non si può eseguire il comando ADDKEY senza digitare la password	

Esempio:

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key /password=<la_tua_password>
```

20.2. Gestione di componenti del programma e attività

Sintassi dei comandi:

```
avp.com <command> <profilo|nome_azione>
avp.com STOP |PAUSE <profile|nome_azione>
/password=<la_tua_password> [/R[A]:<report_file>]
```

Descrizione parametri:

<command>	Puoi gestire i componenti Kaspersky Internet Security e le azioni dal prompt dei comandi

	con i comandi seguenti: **START** – carica un componente di protezione in tempo reale o una azione. **STOP** – arresta un componente di protezione in tempo reale o una azione. **PAUSE** – mette in pausa un componente di protezione in tempo reale o una azione. **RESUME** – riavvia un componente di protezione in tempo reale o una azione. **STATISTICS** – statistica a schermo circa l'operazione del componente di protezione in tempo reale o azione. Notare che non si possono eseguire i comandi PAUSE o STOP senza inserire la password.
<profilo | nome_azione>	È possibile specificare ogni componente di protezione in tempo reale, moduli dei componenti, scansioni su richiesta o aggiornamenti per il valore del **<profilo>** (i valori standard usati nel programma sono mostrati nella tabella sottostante). È possibile specificare il nome ogni scansione su richiesta o aggiornare una azione con il valore del **<nome_azione>**.
<la_tua_password>	La password impostata nell'interfaccia del programma.
/R[A]:<report_file>	**R:<report_file> -** registra solo gli eventi importanti nel report. **/RA:<report_file> -** registra tutti gli eventi nel report. È possibile usare un percorso assoluto o relativo per il file. Se il parametro non è definito i risultati della scansione sono presentati sullo schermo con tutti gli eventi.

A **<profilo>** viene assegnato uno dei seguenti valori:

RTP	Tutti i componenti di protezione. Il comando avp.com START RTP avvia tutti i componenti di protezione in tempo reale se la protezione è completamente disabilitata (vedi 6.1.2 pag. 73 o in pausa (vedi 6.1.1 pag. 72). Questo comando avvierà qualsiasi componente di protezione in tempo reale messo in pausa da GUI o dal comando PAUSE dal prompt dei comandi. Se il componente è stato disabilitato da GUI o dal comando STOP dal prompt dei comandi, il comando avp.com START RTP non lo avvierà. Per avviarlo devi eseguire il comando avp.com START <profilo> digitando per <profilo> il valore per lo specifico componente di protezione.
FM	File Anti-Virus
EM	Mail Anti-Virus
WM	Web Anti-Virus Valori per i sottocomponenti di Web Anti-Virus **httpscan** – scaniona il traffico http **sc** – scansiona gli script
BM	Difesa Proattiva Valori per i sottocomponenti di Difesa Proattiva **pdm** – analisi dell'attività delle applicazioni

ASPY	Controllo Privacy Valori dei subcomponenti per Controllo Privacy **antidial -** Anti-Dialer **antiphishing** – Anti-Phishing **PrivacyControl** – Protegge dati riservati
AH	Firewall Valori dei subcomponenti Firewall **fw** – Sistema di filtro **ids** – Sistema di rilevamento delle intrusioni **AdBlocker** – Anti-pubblicità **popupchk** – Blocco Popup
AS	Anti-Spam
ParCtl	Controllo contenuti
UPDATER	Tool di aggiornamento
Rollback	Ritorno all'aggiornamento precedente
SCAN_OBJECTS	Attività di scansione antivirus
SCAN_MY_COMPUTER	Attività di scansione su Risorse del computer
SCAN_CRITICAL_AREAS	Attività di scansione sulle aree critiche
SCAN_STARTUP	Attività di scansione sugli oggetti di avvio
SCAN_QUARANTENA	Attività di scansione sugli oggetti in Quarantena
SCAN_ROOTKIT	Attività di scansione sui rootkit
I componenti e le azioni avviate dal prompt dei comandi sono eseguiti con le impostazioni configurate nell'interfaccia del programma.	

Esempio:

Per abilitare File Anti-Virus, digitare la seguente stringa nel prompt di comando:

```
avp.com START FM
```

Per visualizzare lo stato corrente di Difesa proattiva sul computer, digitare il testo seguente nel prompt di comando:

```
avp.com STATUS BM
```

Per terminare un'attività di scansione di Risorse del computer dal prompt di comando, digitare:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<la_tua_password>
```

20.3. Scansioni antivirus

L'avvio della scansione antivirus di una determinata area e l'elaborazione degli oggetti nocivi dal prompt di comando generalmente appare così:

```
avp.com SCAN [<oggetto scansionato>] [<azione>]
[<tipo file>] [<esclusione>] [<file configurazione>]
[<impostazioni report>] [<impostazioni avanzate>]
```

Per eseguire la scansione di oggetti è possibile utilizzare anche le attività create in Kaspersky Internet Security avviando quella desiderata dal prompt di comando (vedi 20.1 pag. 314). L'attività viene eseguita con le impostazioni configurate nell'interfaccia del programma.

Descrizione dei parametri:

<object scanned> - questo parametro fornisce un elenco degli oggetti che saranno sottoposti alla scansione in cerca di codici nocivi.

Può includere diversi valori dall'elenco fornito, separati da uno spazio.

<files>	Elenco dei percorsi ai file e/o cartelle da sottoporre a scansione antivirus. È possibile inserire percorsi assoluti o relativi. Gli elementi dell'elenco devono essere separati da uno spazio. Note: Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette. Se si seleziona una cartella specifica, saranno sottoposti a scansione tutti i file in essa contenuti.
/MEMORY	Oggetti della memoria di sistema
/STARTUP	Oggetti ad esecuzione automatica
/MAIL	Database di posta
/REMDRIVES	Tutte le unità rimovibili
/FIXDRIVES	Tutte le unità interne
/NETDRIVES	Tutte le unità di rete
/QUARANTINE	Oggetti in quarantena
/ALL	Scansione completa
/@:<filelist.lst>	Percorso al file con un elenco di oggetti e cartelle inclusi nella scansione. Il file deve essere in formato testo e ogni oggetto della scansione deve essere a capo riga. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere inserito tra virgolette se contiene uno spazio.
<azione> - questo parametro imposta le reazioni agli oggetti nocivi rilevati durante la scansione. Se questo parametro non è definito, l'azione predefinita è quella con il valore per **/i8**.	

/i0	Nessuna azione sull'oggetto; solo registrazione delle informazioni nel report.
/i1	Trattare gli oggetti infetti e, se la riparazione non riesce, ignorare.
/i2	Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminare, ma non eliminare gli oggetti appartenenti ad oggetti composti, ed eliminare gli oggetti composti con intestazione eseguibile (archivi sfx) (impostazione predefinita).
/i3	Trattare gli oggetti infetti e, se la riparazione non riesce, eliminare, ed eliminare completamente tutti gli oggetti composti se non si riesce ad eliminare l'allegato infetto.
/i4	Eliminare gli oggetti infetti e, se la riparazione non riesce, eliminare. Inoltre eliminare completamente tutti gli oggetti compositi se non si riesce ad eliminare il contenuto infetto.
/i8	Avvisa l'utente di intraprendere una azione se viene riconosciuto un oggetto infetto.
/i9	Avvisa l'utente di intraprendere una azione alla fine della scansione.
<tipo_file> - questo parametro definisce il tipo di file soggetti a scansione anti-virus. Se il parametro non è definito, il valore predefinito è /fi.	
/fe	Esaminare solo i file potenzialmente infetti in base all'estensione
/fi	Esaminare solo i file potenzialmente infetti in base ai contenuti
/fa	Esaminare tutti i file

<exclusion> - questo parametro definisce gli oggetti da escludere dalla scansione.

Può includere diversi valori dall'elenco fornito, separati da uno spazio.

-e:a	Non esaminare archivi
-e:b	Non esaminare i database di posta
-e:m	Non esaminare i messaggi di testo semplice
-e:<filemask>	Non esaminare oggetti in base alle maschere.
-e:<seconds>	Ignorare oggetti esaminati più a lungo del tempo specificato dal parametro <secondi>
-es:<dimensione>	Ignora i file più grandi (in MB) del valore impostato per <dimensione>

<configuration file> - questo parametro definisce il percorso al file di configurazione che contiene le impostazioni del programma per la scansione.

Il file di configurazione è un file in formato testo che contiene un set di parametri per la linea di comando della scansione anti-virus.

È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono applicati i valori impostati dall'interfaccia di Kaspersky Internet Security.

/C:<nome_file>	Usare i valori delle impostazioni assegnati nel file **<nome_file>**

<report Impostazioni> - questo parametro definisce il formato del report sui risultati della scansione.

È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, vengono visualizzati i risultati della scansione e tutti gli eventi.

/R:<report_file>	Registrare in questo file solo gli eventi importanti
/RA:<report_file>	Registrare tutti gli eventi in questo file

<impostazioni avanzate> - impostazioni che definiscono l'uso delle tecnologie di scansione anti-virus.

/iChecker=<on|off>	Abilita/Disabilita iChecker
/iSwift=<on|off>	Abilita/Disabilita iSwift

Esempio:

avvio di una scansione della RAM, programmi ad esecuzione automatica, database di posta, le directory **Documenti** e **Programmi***, e il file* **test.exe***:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Impostazioni\All Users\My Documents" "C:\Program
Files" "C:\Downloads\test.exe"
```

Sospensione temporanea della scansione di oggetti selezionati e avvio di una scansione completa del computer, quindi proseguimento della scansione antivirus degli oggetti selezionati:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Scansione RAM e degli oggetti elencati nel file ***object2scan.txt****. Uso del file di configurazione* ***scan_setting.txt****. Dopo la scansione, creazione di un report con registrazione di tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_Impostazioni.txt /RA:scan.log
```

Esempio di file di configurazione:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

20.4. Aggiornamenti del programma

La sintassi per l'aggiornamento dei moduli di Kaspersky Internet Security e dei database dal prompt di comando è la seguente:

```
avp.com UPDATE [<aggiorna_fonte>]
[/R[A]:<fiel_report>] [/C:<nome_file>] [/APP=<on |
off>]
```

Descrizione dei parametri:

[<aggiorna_fonte>]	Server HTTP o FTP o cartella di rete per il prelievo degli aggiornamenti. Come valore del parametro è possibile specificare il percorso completo o l'URL per la fonte di aggiornamento. In assenza di un percorso selezionato, la fonte di aggiornamento sarà quella delle impostazioni di Aggiornamento.
/R[A]:<report_file>	**/R:<report_file>** – registrare solo gli eventi importanti nel report. **/R[A]:<report_file>** – registrare tutti gli eventi nel report. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, vengono visualizzati i risultati della scansione e tutti gli eventi.
/C:<nome_file>	Percorso al file di configurazione con le impostazioni degli aggiornamenti del programma. Il file di configurazione è un file in formato testo che contiene un set di parametri per la riga di comando per l'aggiornamento dell'applicazione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono applicati i valori impostati dall'interfaccia di Kaspersky Internet Security.
/APP=<on | off>	Abilita / Disabilita gli aggiornamenti dei moduli del programma

Esempio:

Aggiornamento degli elenchi delle minacce dopo la registrazione di tutti gli eventi nel report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

Aggiornamento dei moduli di Kaspersky Internet Security applicando le impostazioni nel file di configurazione ***updateapp.ini****:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

Esempio del file di configurazione:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

20.5. Impostazioni di ritorno

Sintassi del comando:

```
ROLLBACK [/R[A]:<report_file>] [/password=<password>]
```

/R[A]:<report_file>	/R:<report_file> - registra nel report solo gli eventi importanti /RA:<report_file> - registra nel report tutti gli eventi. È possibile indicare un percorso assoluto o relativo. Se il parametro non è impostato i risultati della scansione e tutti gli eventi saranno presentati sullo schermo.
<password>	Password per accedere a Kaspersky Internet Security impostata nell'interfaccia dell'applicazione.
Notare che non si può eseguire questo comando senza digitare la password.	

Esempio:

```
avp.com ROLLBACK /RA:rollback.txt
/password=<la_tua_password>
```

20.6. Esportazione delle impostazioni di protezione

Sintassi dei comandi:

```
avp.com EXPORT <profile > <nome_file>
```

Descrizione dei parametri:

<profile>	Componente o attività le cui impostazioni vengono esportate. Può essere usato uno dei valori elencati in 20.2 a pag. 314

<nome_file>	Percorso al file su cui sono esportate le impostazioni di Kaspersky Internet Security. È possibile inserire percorsi assoluti o relativi. Il file di configurazione è salvato in formato binario (.dat) e può essere usato in seguito per importare le impostazioni dell'applicazione su altri computer. Il file di configurazione può essere salvato come file testo. A tal fine, specificare l'estensione .txt nel nome del file. Questo file può essere utilizzato solo per specificare le principali impostazioni per l'operatività del programma.

Esempio:

```
avp.com EXPORT c:\settings.dat
```

20.7. Importazione delle impostazioni

Sintassi dei comandi:

```
avp.com IMPORT <nome_file> [/password=<password>]
```

<nome_file>	Percorso al file da cui sono importate le impostazioni di Kaspersky Internet Security. È possibile inserire percorsi assoluti o relativi. Le impostazioni possono essere importate solo da file binari.
<la_tua_password>	La password di Kaspersky Internet Security impostata nell'interfaccia del programma.
Notare che non si può eseguire questo comando senza inserire la password.	

Esempio:

```
avp.com IMPORT c:\settings.dat /password=<password>
```

20.8. Avvio del programma

Sintassi dei comandi:

```
avp.com
```

20.9. Arresto del programma

Sintassi dei comandi:

```
EXIT /password=<la_tua_password>
```

<password>	La password di Kaspersky Internet Security impostata dall'interfaccia del programma.
Notare che non si può eseguire questo comando senza inserire la password.	

Osservare che non è possibile eseguire questo comando senza digitare la password.

20.10. Creazione di un file di tracciato

Potrebbe essere necessario creare un file di tracciato in caso di problemi con il programma da approfondire con gli specialisti del Supporto Tecnico.

Sintassi dei comandi:

```
avp.com TRACE [file] [on|off] [<trace_level>]
```

Descrizione dei parametri:

[on|off]	Abilita/Disabilita la creazione del tracciato.
[file]	File del tracciato.

<trace_level>	Questo parametro può essere un numero tra 0 (livello minimo, solo messaggi critici) e 700 (livello massimo, tutti i messaggi). Il Supporto Tecncio indicherà il livello corretto. Se non viene specificato consigliamo di impostarlo su 500.

Attenzione!

Consigliamo di creare un file di tracciato solo per specifici problemi. L'abilitazione regolare della tracciatura potrebbe rallentare il computer e saturare il disco fisso.

Esempio:

Per disabilitare la creazione di un tracciato:

```
avp.com TRACE file off
```

Per creare un file di tracciato ed inviarlo al Supporto Tecnico con un livello massimo impostato a 500:

```
avp.com TRACE file on 500
```

20.11. Visualizzazione della Guida

Questo comando è disponibile per visualizzare la Guida con la sintassi del prompt di comando:

```
avp.com [ /? | HELP ]
```

Per ricevere aiuto sulla sintassi di un comando specifico, è possibile usare uno dei seguenti comandi:

```
avp.com <command> /?
avp.com HELP <command>
```

20.12. Codici di ritorno dall'interfaccia della riga di comando

Questa sezione contiene un elenco di codici di ritorno dalla riga di comando. Codici generici possono sempre essere ritornati da qualsiasi comando della riga

di comando. I codici di ritorno includono codici generici e codici specifici per speficici tipi di azioni.

Codici di ritorno generici	
0	Operazione completata con successo
1	Valore di impostazione non valido
2	Errore sconosciuto
3	Errore nel completamento dell'azione
4	Azione cancellata
Codici di ritorno delle scansioni anti-virus	
101	Processati tutti gli oggetti pericolosi
102	Rinvenuti oggetti pericolosi

CAPITOLO 21. MODIFICA, RIPARAZIONE E DISINSTALLAZIONE DEL PROGRAMMA

L'applicazione può essere disinstallata in due modi:

- usando la procedura guidata di installazione (vedi 21.2 pag. 331)
- dal prompt di comando (vedi 21.2 pag. 331)

21.1. Modifica, riparazione e rimozione del programma con la procedura guidata di installazione

In caso di errori di funzionamento dovuti a un'errata configurazione o alla corruzione dei file può rendersi necessario riparare il programma.

La modifica del programma consente di installare componenti di Kaspersky Internet Security assenti o di eliminare quelli che non si desiderano.

Per riparare o modificare i componenti assenti di Kaspersky Internet Security o disinstallare il programma:

1. Inserire l'eventuale CD di installazione nell'unità CD-ROM (se utilizzato per installare il programma). Se Kaspersky Internet Security è stato installato da una diversa origine (cartella ad accesso pubblico, cartella nel disco fisso, ecc.), verificare che la cartella contenga il pacchetto di installazione e di potervi accedere.
2. Selezionare **Start → Tutti i programmi → Kaspersky Internet Security 7.0 → Modifica, Ripara o Rimuovi**.

Si apre una procedura di installazione guidata del programma. Osserviamo in dettaglio i passaggi necessari per riparare, modificare o eliminare il programma.

Passaggio 1. Selezione di un'operazione

In questa fase è richiesto di selezionare l'operazione che si desidera eseguire. È possibile modificare i componenti del programma, riparare i componenti già installati o rimuovere dei componenti o l'intero programma. Per eseguire l'operazione desiderata, fare clic sul pulsante appropriato. La reazione del programma dipende dall'operazione selezionata.

La modifica del programma è analoga all'installazione personalizzata, in cui è possibile specificare quali componenti si desidera installare e quali eliminare.

La riparazione del programma dipende dai componenti installati. Saranno riparati i file di tutti i componenti installati e per ciascuno di essi sarà impostato il livello di sicurezza Raccomandato.

Se si rimuove il programma, è possibile selezionare quali dati creati e usati dal programma si desidera salvare sul computer. Per eliminare tutti i dati di Kaspersky Internet Security, selezionare **Disinstallazione completa**. Per salvare i dati, selezionare **Salva oggetti applicazione** e specificare quali oggetti non eliminare:

- *Dati attivazione* – il file della chiave dell'applicazione.
- *Database dell'applicazione* – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti all'ultimo aggiornamento.
- *Database di Anti-Spam* – database utilizzato per individuare la posta indesiderata. Questo database contiene informazioni dettagliate su quali messaggi costituiscono spam e quali no.
- *File di backup* – copie di backup di oggetti eliminati o riparati Si raccomanda di salvarli per poterli eventualmente ripristinare in un secondo momento.
- *File in Quarantena* – file potenzialmente infetti da virus o varianti di essi. Questi file contengono codici simili a quelli di virus noti ma è difficile stabilire se siano nocivi. Si raccomanda di salvare questi file poiché potrebbero essere normali o riparati dopo l'aggiornamento dei database.
- *Impostazioni della protezione* – configurazioni per tutti i componenti del programma.
- *Dati iSwift* – database con informazioni sugli oggetti esaminati nel file system NTFS. Può accelerare la scansione. Quando usa questo database, Kaspersky Internet Security esamina solo i file che hanno subito modifiche in seguito all'ultima scansione.

Attenzione!

Se trascorre un lungo periodo tra la disinstallazione di una versione di Kaspersky Internet Security e l'installazione di un'altra, si sconsiglia di utilizzare il database *iSwift* di una versione precedente. Un programma pericoloso potrebbe essere penetrato nel computer nel frattempo e i suoi effetti non sarebbero rilevati dal database, con conseguente rischio di infezione.

Per avviare l'operazione selezionata fare clic sul pulsante **Avanti**. Il programma inizia a copiare i file necessari sul computer o a eliminare i componenti e i dati selezionati.

Passaggio 2. Completamento della modifica, riparazione o rimozione del programma

L'avanzamento del processo di modifica, riparazione o rimozione del programma viene seguito sullo schermo. Al termine l'utente sarà informato del completamento dell'operazione.

La rimozione del programma richiede solitamente il riavvio del computer, necessario per applicare le modifiche al sistema. Il programma chiede quindi se si desidera riavviare il computer. Fare clic su **Sì** per riavviarlo subito. Per riavviarlo in un secondo momento, scegliere invece **No**.

21.2. Disinstallazione del programma dalla riga di comando

Per disinstallare Kaspersky Internet Security dal computer, digitare:

```
msiexec /x <package_name>
```

Si apre la procedura guidata di installazione, che può essere usata per disinstallare l'applicazione (vedi Capitolo 21 pag. 329).

Si può anche usare la riga di comando sottostante.

Per disinstallare l'applicazione in background senza riavviare il computer (il computer dovrebbe essere riavviato manualmente dopo la disinstallazione), digita:

```
msiexec /x <package_name> /qn
```

Per disinstallare l'applicazione in background e quindi riavviare il computer, digita:

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

CAPITOLO 22. DOMANDE FREQUENTI

Questo capitolo è dedicato alle domande più frequenti poste dai nostri utenti sull'installazione, la configurazione e il funzionamento di Kaspersky Internet Security; faremo il possibile per fornire risposte più esaurienti possibile.

Domanda: È possibile usare Kaspersky Internet Security 7.0 con prodotti antivirus di altri fabbricanti?

No. Si raccomanda di disinstallare altri prodotti antivirus eventualmente presenti sul computer prima di installare Kaspersky Internet Security per evitare conflitti di software.

Domanda: Kaspersky Internet Security non riesamina i file precedentemente sottoposti alla scansione. Perché?

È vero. Kaspersky Internet Security non riesamina i file che non hanno subito variazioni dalla scansione precedente.

Ciò è possibile grazie alle nuove tecnologie iChecker e iSwift. La tecnologia viene implementata nel programma utilizzando un database di checksum dei file e un archivio di checksum dei file in flussi NTFS alternati.

Domanda: Perché occorre una chiave di licenza? Kaspersky Internet Security non funziona senza?

Kaspersky Internet Security funziona anche senza chiave di licenza ma il programma non è in grado di accedere al modulo di aggiornamento e al supporto tecnico.

Se non si è ancora deciso se acquistare Kaspersky Internet Security, possiamo fornire una chiave di licenza in prova per due settimane o un mese. Trascorso questo periodo, la chiave scade.

Domanda: Dopo l'installazione di Kaspersky Internet Security il sistema operativo ha iniziato a "comportarsi" in maniera strana (schermo blu, riavvii frequenti, ecc.). Cosa devo fare?

Sebbene si tratti di una circostanza rara, è possibile che Kaspersky Internet Security e altri software presenti sul computer siano in conflitto.

Per ripristinare la funzionalità del sistema operativo procedere come segue:

1. Premere il tasto **F8** non appena il computer inizia a caricarsi fino a visualizzare il menu di avvio.
2. Selezionare la **Modalità provvisoria** e caricare il sistema operativo.
3. Aprire Kaspersky Internet Security.
4. Aprire la finestra principale dell'applicazione e selezionare la sezione **Servizio**.
5. Deselezionare **Lancia l'applicazione all'avvio** e fare clic su **OK**.
6. Riavviare il sistema operativo in modalità regolare.

Inviare una richiesta al Supporto Tecnico di Kaspersky Lab. Aprire la finestra principale dell'applicazione, selezionare **Supporto** e cliccare su **Sottoporre una domanda**. Descrivere il problema e la sua firma nel più dettagliato modo possibile.

Ricordare di allegare alla domanda un file contenente un'immagine completa della memoria del sistema operativo Microsoft Windows. Per creare questo file procedere come segue:

1. Fare clic con il pulsante destro del mouse su **Risorse del computer** e selezionare l'elemento **Proprietà** del menu di scelta rapida che si apre.
2. Selezionare la scheda **Avanzate** nella finestra **Proprietà del sistema**, quindi premere il pulsante **Impostazioni** nella sezione **Avvio e ripristino**.
3. Selezionare l'opzione **Immagine della memoria completa** dal menu a discesa della sezione **Scrivi informazioni di debug** nella finestra **Avvio e ripristino**.

   Per impostazione predefinita, il file dell'immagine della memoria viene salvato nella cartella di sistema come *memory.dmp*. È possibile modificare la cartella di salvataggio dell'immagine rinominando la cartella nel campo corrispondente.
4. Riprodurre il problema relativo al funzionamento di Kaspersky Internet Security.
5. Accertarsi che l'immagine completa della memoria sia stata salvata correttamente.

APPENDICE A. RIFERIMENTI

Questa appendice contiene materiale di riferimento sui formati dei file e le maschere delle estensioni utilizzate nelle impostazioni di Kaspersky Internet Security.

A.1. Elenco dei file esaminati in base all'estensione

Se si seleziona **Esamina programmi e documenti (in base all'estensione)**, File Anti-Virus sottopone a un'approfondita scansione antivirus i file con le estensioni sotto elencate. Se si abilita il filtro degli allegati, anche Mail Anti-Virus esaminerà questi file.

com – file eseguibile di un programma

exe – file eseguibile o archivio autoestraente

sys – file di sistema

prg – testo di programma per dBase, Clipper o Microsoft Visual FoxPro, o programma di WAVmaker

bin – file binario

bat – file batch

cmd – file di comando per Microsoft Windows NT (simile a un file .bat per DOS), OS/2

dpl – libreria compressa Borland Delphi

dll – libreria di caricamento dinamico

scr – splash screen di Microsoft Windows

cpl – modulo del pannello di controllo di Microsoft Windows

ocx – oggetto Microsoft OLE (Object Linking and Embedding)

tsp – programma eseguito in modalità split-time

drv – driver di periferica

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – file link di Microsoft Windows

reg – file della chiave di registro del sistema di Microsoft Windows

ini – file di inizializzazione

cla – classe Java

vbs – Visual Basic script

vbe – estensione video BIOS

js, jse – testo origine JavaScript

htm – documento ipertestuale

htt – intestazione ipertesto di Microsoft Windows

hta – file di ipertesto usato per aggiornare il registro del sistema operativo

asp – script Active Server Pages

chm – file HTML compilato

pht – HTML con script PHP incorporati

php – script incorporato in file HTML

wsh – file Microsoft Windows Script Host

wsf – script Microsoft Windows

the – wallpaper di Microsoft Windows 95

hlp – file Win Help

eml – file di posta di Microsoft Outlook Express

nws – nuovo file di posta di Microsoft Outlook Express

msg – file di posta Microsoft Mail

plg – e-mail

mbx – estensione dei messaggi di Microsoft Office Outlook salvati

*doc** – documento di Microsoft Office Word, come : *doc* – Documento di Microsoft Office Word, *docx* – Documento di Microsoft Office Word 2007 con supporto XML, *docm* – Documento di Microsoft Office Word 2007 con supporto di macro.

*dot **– modello di documento di Microsoft Office Word, come *dot* – Modello di documento di Microsoft Office Word, *dotx* – Modello di documento di Microsoft Office Word 2007, *dotm* – Modello di documento di Microsoft Office Word 2007 con supporto macro.

doc – documento di Microsoft Office Word

dot – modello di documento di Microsoft Office Word

fpm – programma di database, file di avvio di Microsoft Visual FoxPro

rtf – documento Rich Text Format

shs – frammento Shell Scrap Object Handler

dwg – database blueprint AutoCAD

msi – pacchetto Microsoft Windows Installer

otm – progetto VBA per Microsoft Office Outlook

pdf – documento di Adobe Acrobat

swf – file Shockwave Flash

jpg, jpeg, png – formato immagini compresso

emf – formato Enhanced Metafile, la prossima generazione di metafile per Microsoft Windows OS. I file EMF non sono supportati da Microsoft Windows a 16 bit.

ico – icona di un programma

ov? – file eseguibili MS DOC

*xl** - Documenti e file di Microsoft Office Excel come,: *xla* – add-on di Microsoft Office Excel , *xlc* – diagramma, *xlt* – modello documento, *xlsx* – workbook di Microsoft Office Excel 2007 , *xltm* – workbook di Microsoft Office Excel 2007 con supporto macro, *xlsb* – Microsoft Office Excel 2007 in formato binario (non XML), *xltx* – modello di Microsoft Office Excel 2007, *xlsm* – modello di Microsoft Office Excel 2007 con supporto macro, *xlam* – add-on di Microsoft Office Excel 2007 con supporto macro.

*pp** - Documenti e file di Microsoft Office PowerPoint come: *pps* – diapositiva di Microsoft Office PowerPoint, *ppt* – presentazione, *pptx* – presentazione di Microsoft Office PowerPoint 2007, *pptm* – presentazione di Microsoft Office PowerPoint 2007 con supporto macro, *potx* – modello di presentazione di Microsoft Office PowerPoint 2007, *potm* – modello di presentazione di Microsoft Office PowerPoint 2007 con supporto macro, *ppsx* – diapositive di Microsoft Office PowerPoint 2007, *ppsm* – diapositive di Microsoft Office PowerPoint 2007 con supporto macro, *ppam* – add-on di Microsoft Office PowerPoint 2007 con supporto macro.

*md** – Documenti e file di Microsoft Office Access, come *mda* – workgroup di Microsoft Office Access, mdb – database, ecc.

sldm – diapositiva di Microsoft PowerPoint 2007 con supporto macro.

thmx – Tema di Microsoft Office 2007.

Ricordare che il formato effettivo di un file può non corrispondere al formato indicato dall'estensione.

A.2. Maschere di esclusione file valide

Osserviamo alcuni esempi delle maschere possibili per la creazione di elenchi di esclusione di file:

1. Maschere senza percorso file:
   - ***.exe** – tutti i file con estensione exe
   - ***.ex?** – tutti i file con estensione *.ex?,* dove ? può rappresentare qualsiasi carattere singolo

- **test** – tutti i file di nome *test*

2. Maschere con percorso file assoluto:
   - **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file nella cartella *C:\dir*
   - **C:\dir*.exe** – tutti i file con estensione *.exe* contenuti nella cartella C:\dir\
   - **C:\dir*.ex?** – tutti i file con estensione *.ex?* nella cartella *C:\dir*, in cui ? è utilizzato in sostituzione di un carattere
   - **C:\dir\test** – solo il file *C:\dir\test*

     Se non si desidera che il programma esamini i file nelle sottocartelle di questa cartella, selezionare **Includi sottocartelle** durante la creazione della maschera.
3. Maschere con percorso file relativo:
   - **dir*.*** o **dir*** o **dir** – tutti i file in tutte le cartelle *dir*
   - **dir\test** – tutti i file *test* nelle cartelle *dir*
   - **dir*.exe** – tutti i file con estensione *.exe* in tutte le cartelle in *dir*
   - **dir*.ex?** – tutti i file con estensione *.ex?* in tutte le cartelle di *C:\dir*, in cui ? è utilizzato in sostituzione di un carattere

     Se non si desidera che il programma esamini i file nelle sottocartelle di questa cartella, selezionare **Includi sottocartelle** durante la creazione della maschera.

Suggerimento:

Le maschere di esclusione *.* e * possono essere usate esclusivamente se si assegna l'esclusione ad un tipo di minaccia in accordo con l'Enciclopedia dei Virus. In caso contrario, la minaccia specificata non sarà rilevata in alcun oggetto. L'uso di queste maschere senza selezionare il tipo di minaccia disabilita il monitoraggio.

Si sconsiglia inoltre di selezionare un'unità virtuale creata sulla base di una directory di file system usando il comando *subst* come esclusione. Non avrebbe alcun senso farlo poiché, durante la scansione, il programma percepisce questa unità virtuale come cartella e di conseguenza la esamina.

A.3. Maschere di esclusione valide in base alla classificazione dall'Enciclopedia dei Virus

Durante l'aggiunta di minacce con un determinato stato dalla classificazione dell'enciclopedia dei virus come esclusioni, è possibile specificare:

- Il nome completo della minaccia come indicato nell'enciclopedia dei virus all'indirizzo www.viruslist.com (per esempio, **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**);
- Il nome della minaccia mediante maschera. Ad esempio:
  - **not-a-virus*** – esclude dalla scansione potenziali programmi pericolosi e programmi scherzo.
  - ***Riskware.*** – esclude dalla scansione i riskware.
  - ***RemoteAdmin.*** – esclude dalla scansione tutti i programmi di amministrazione remota.

APPENDICE B. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è diventata un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non sollecitati e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un'azienda internazionale con sede nella Federazione Russia e rappresentanti nel Regno Unito, Francia, Germania, Giappone, USA (CA), Benelux, Cina, Polonia e Romania. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 450 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e vari membri della Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus consente all'azienda di offrire una protezione completa contro minacce presenti e future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e commerciali.

Anni di duro lavoro ne hanno fatto un'azienda leader tra i principali produttori di software per la sicurezza informatica. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard della protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Internet Security, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, server di file, sistemi di posta elettronica, firewall e gateway di Internet e computer portatili. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'impresa. Numerose imprese di grande notorietà si affidano a Kaspersky Internet Security, per esempio Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di una vasta serie di servizi supplementari volti a garantire sia un funzionamento stabile dei prodotti dell'azienda, sia la conformità a qualsiasi esigenza aziendale specifica. Il database antivirus di Kaspersky Lab viene aggiornato ogni ora. L'azienda offre ai

propri clienti un servizio di assistenza tecnica 24 ore su 24, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

B.1. Altri prodotti Kaspersky Lab

News Agent di Kaspersky Lab

News Agent è progettato per comunicare tempestivamente le notizie pubblicate da Kaspersky Lab, per le notifiche relative allo stato corrente dell'attività dei virus e per notizie fresche. Il programma legge l'elenco dei canali news disponibili e il loro contenuto dai server di notizie di Kaspersky Lab con la frequenza specificata.

News Agent abilita l'utente a:

- Visualizza nella barra di sistema lo previsione corrente dei virus
- Il prodotto consente di iscriversi e cancellarsi dai canali news
- Recupera le notizie da ogni canale selezionato con la frequenza specificata e informa sulle ultime notizie
- Consente di consultare le notizie sui canali selezionati
- Consente di consultare l'elenco dei canali e il loro stato
- Consente di aprire nel browser pagine con articoli completi

News Agent è un'applicazione Microsoft Windows stand-alone che può essere utilizzata da sola o con varie soluzioni integrate offerte da Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Questo programma è un servizio gratuito offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer. Kaspersky OnLine Scanner funziona direttamente dal tuo browser. Gli utenti hanno così ottenere una veloce risposta riguardo le potenziali infezioni del loro computer. Con questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta
- Selezionare per la scansione dei database standard/estesi
- Salvare un report dei risultati di scansione in formato txt o html

Kaspersky® OnLine Scanner Pro

Questo programma è un servizio a pagamento offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer e di riparare i file pericolosi. Kaspersky OnLine Scanner Pro funziona direttamente dal tuo browser . Grazie a questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta
- Selezionare per la scansione database antivirus standard/estesi
- Salvare un report dei risultati di scansione in formato txt o html

Kaspersky® Anti-Virus 7.0

Kaspersky Anti-Virus 7.0 è progettato per proteggere i personal computer dal software nocivo grazie a una combinazione ottimale di metodi di protezione antivirus convenzionali e nuove tecnologie proattive.

Il programma offre complesse verifiche antivirus fra cui:

- Scansione antivirus del traffico e-mail al livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in arrivo, e SMTP per quella in uscita) indipendentemente dal client di posta usato, nonché riparazione dei database di posta.
- Scansione antivirus in tempo reale del traffico Internet trasferito mediante HTTP.
- Scansione antivirus di singoli file, directory o unità. Inoltre è possibile usare un'attività di scansione preimpostata per iniziare l'analisi antivirus esclusivamente delle aree critiche del sistema operativo e degli oggetti di avvio di Microsoft Windows.

La protezione proattiva offre le seguenti funzioni:

- *Controllo delle modifiche del file system*. Il programma consente agli utenti di creare un elenco di applicazioni che controllerà in base ai componenti. Aiuta a proteggere l'integrità delle applicazioni dall'influsso del software nocivo.
- *Monitoraggio dei processi nella RAM*. Kaspersky Anti-Virus 7.0 avvisa tempestivamente gli utenti ogni volta che rileva processi pericolosi, sospetti o nascosti, o nei casi in cui si siano verificate variazioni non autorizzate dei processi standard.
- *Monitoraggio delle variazioni del registro OS* dovute al controllo del registro interno del sistema.
- *Monitoraggio dei processi nascosti* protegge dai codici maligni nascosti nel sistema operativo usando la tecnologie rootkit.
- *Analizzatore Euristico* durante la scansione di un programma, l'analizzatore simula la sua esecuzione e registra tutte le attività sospette come aprire o scrivere su un file, interrompere l'intercettazione di vettori etc. Sulla base di questa procedura decide riguardo la possibile infezione con un virus del programma. La simulazione avviene in un ambiente che con affidabilità protegge il computer dall'infezione.

- *Ripristino del sistema in seguito* ai danni provocati da malware registrando tutte le variazioni del registro e del file system del computer, e permettendo, a discrezione dell'utente, il ritorno ad una versione precedente.

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile fornisce una protezione per apparati mobili funzionanti con Symbian OS e Microsoft Windows Mobile. Il programma assicura una scansione esaustiva comprendente:

- *Scansione su richiesta* della memoria dell'apparato, memory cards o cartelle individuali o uno specifico file; se viene rilevato un file infetto questo viene spostato in Quarantena o eliminato
- *Scansione real-time* – tutti i file in ingresso ed uscita sono scansionati automaticamente, come pure i file oggetti di tentativi di accesso
- *Protezione da spam* contenuto nei messaggi di testo

Kaspersky Anti-Virus for file server Questo pacchetto fornisce una affidabile protezione da tutti i tipi di malware per i file di sistema su server che operano con Microsoft Windows, Novell NetWare, Linux e Samba. La suite include le seguenti applicazioni Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Caratteristiche e funzionalità:

- *Protegge i file system dei server in tempo reale*. Tutti i file dei server sono scansionati quando aperti o salvati sul server;
- *Evita l'epidemia virus;*
- *Scansione su richiesta* dell'intero file system o di file o cartelle individuali;
- *Usa tecnologie di ottimizzazione* nella scansione degli oggetti nel file system del server;
- *Possibilità di rollback dopo un attacco virus;*
- *Scalabilità del pacchetto software* in accordo con la capacità delle risorse disponibili di sistema;
- *Monitoraggio del sistema di cattivo billanciamento;*

- *Creazione di un elenco di processi sicuri* la cui attività sul server non è soggetta a controllo dal pacchetto software;
- *Amministrazione remota del pacchetto software*, compreso installazione, configurazione ed amministrazione centralizzata;
- *Salvataggio di copie di backup degli oggetti infettati o cancellati* nel caso tu abbia bisogno di ripristinarle;
- *Messa in Quarantena degli oggetti sospetti;*
- *Invio di notifiche degli eventi nell'esecuzione* del programma all'amministratore di sistema;
- *Registrazione di dettagliati report;*
- *Aggiornamento* automatico dei database del programma.

Sicurezza Kaspersky Open Space

Kaspersky Open Space Security è un pacchetto software con un nuovo approccio alla sicurezza per le rete aziendali attuali di qualsiasi dimensione assicurando un sistema informativo di protezione centralizzato ed il supporto per uffici remoti e utenti in movimento.

La suite comprende quattro programmi:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifiche per ogni programma sono fornite di seguito.

Kaspersky WorkSpace Security è un programma per la protezione centralizzata di workstation interne ed esterne alla rete aziendale contro tutte le minacce attuali di Internet (virus, spyware, attacchi di hacker e spam).

Caratteristiche e funzionalità:

- *Affidabile protezione da virus, spyware, attacchi hacker e spam;*
- *Difesa Proattiva* da nuovi programmi maligni le cui firme non sono ancora state aggiunte al database;
- *Firewall personale* con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete;
- *Rollback per modifiche pericolose del sistema;*
- *Protezione dagli attacchi phishing mail indesiderate;*

- *Ridistribuzione dinamica delle risorse durante la completa scansione del sistema;*
- *Amministrazione Remota* del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata;
- *Supporto per Cisco® NAC* (Network Admission Control);
- *Scansione e-mail e traffico Internet* in tempo reale, blocco delle finestre pop-up e banner pubblicitari su Internet;
- *Operatività sicura in qualsiasi tipo di Network* compreso Wi-Fi;
- *Creazione del disco di emergenza* per poter ripristinare il sistema dopo una invasione virus;
- *Ampio sistema di reportistica* sugli stati della protezione;
- *Aggiornamento automatico dei database;*
- *Supporto completo per sistemi operativi a 64-bit;*
- *Ottimizzazione* delle prestazioni del programma su laptop (tecnologia Intel® Centrino® Duo);
- *Capacità di disinfezione remota* (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security fornisce una ottima protezione alle risorse informative aziendali dalle odierne minacce Internet. Kaspersky Business Space Security protegge workstation e file server da tutti i tipi di virus, Trojan e worm, impedisce la diffusione dei virus ed assicura le informazioni mentre garantisce un accesso immediato alle risorse di rete per l'utente.

Caratteristiche e funzionalità:

- Amministrazione Remota del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata;
- *Supporto per Cisco® NAC* (Network Admission Control);
- *Protezione di workstation e file server da tutti i tipi di minacce;*
- *tecnologia iSwift per evitare la ripetizione della scansione file internamente alla rete;*
- *Distribuzione del carico tra i server;*
- *Oggetti sospetti in Quarantena da workstation;*
- *Rollback per modifiche pericolose del sistema;*

- *Scalabilità del pacchetto software* in accordo con la capacità delle risorse disponibili di sistema;
- *Difesa Proattiva* per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database;
- *Scansione e-mail e traffico internet in tempo reale;*
- *Firewall personale* con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete;
- *Protezione mentre si usa* un network Wi-Fi;
- *Auto-Difesa da programmi maligni;*
- *Oggetti sospetti in Quarantena;*
- *Aggiornamento automatico dei database.*

Kaspersky Enterprise Space Security

Questo programma comprende componenti per la protezione dalle attuali minacce Internet collegati a workstation e server. Cancella i virus dalle e-mail, rendendo sicura l'informazione mentre fornisce un accesso sicuro alle risorse di rete per l'utente.

Caratteristiche e funzionalità:

- *Protezione delle workstation e file server da virus, Trojan e worm;*
- *Protezione di server di posta Sendmail, Qmail, Postfix e Exim;*
- *Scansione di tutte le e-mail su microsoft Exchange Server* compreso le cartelle condivise;
- *Processo di tutte le e-mail, database ed altri oggetti per i server Lotus Domino;*
- *Protezione dagli attacchi phishing e junk mail;*
- *Prevenzione infezione virus e mass mailing;*
- *Scalabilità del pacchetto software* in accordo con la capacità delle risorse disponibili di sistema;
- *Amministrazione Remota* del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata;
- *Supporto per Cisco® NAC* (Network Admission Control);
- *Difesa Proattiva* per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database;

- *Firewall personale* con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete;
- *Protezione sicura mentre si usa* un network Wi-Fi;
- *Scansione traffico* Internet in tempo reale;
- *Rollback* per modifiche pericolose del sistema;
- *Ridistribuzione dinamica delle risorse durante* la completa scansione del sistema;
- *Oggetti sospetti in Quarantena;*
- *Ampio sistema di reportistica sugli stati della protezione;*
- *Aggiornamento automatico dei database.*

Kaspersky Total Space Security

Questo programma esegue il monitoraggio del flusso dati in ingresso ed uscita (e-mail,Internet e tutte le interazioni di rete). Comprende i componenti per la protezione di workstation ed apparati mobili,mantenendo sicura l'informazione mentre fornisce per l'utente un accesso sicuro alle risorse informative della rete aziendale e di Internet e una sicura comunicazione via e-mail.

Caratteristiche e funzionalità:

- *Protezione completa da virus, spyware, attacchi hacker e spam* a qualsiasi livello della rete aziendale da workstation a gateway Internet;
- *Difesa Proattiva* per workstation da programmi maligni le cui firme non sono ancora state aggiunte ai database;
- *Protezione dei server di posta e server collegati;*
- *Scansione del traffico Internet* (HTTP/FTP) in tempo reale sull'area del network locale;
- *Scalabilità del pacchetto software* in accordo con la capacità delle risorse disponibili di sistema;
- *Blocco degli accessi da workstation infettate;*
- *Prevenzione epidemia virus;*
- *Reportistica centralizzata sugli stati di protezione;*
- *Amministrazione Remota* del pacchetto software, comprendente installazione, configurazione ed amministrazione centralizzata;
- *Supporto per Cisco® NAC* (Network Admission Control);

- *Supporto per hardware server proxy;*
- *Filtro del traffico Internet* usando elenchi di server, tipi di oggetto e gruppi di utenti sicuri;
- *Tecnologia iSwift per evitare la ripetizione della scansione di file nella rete;*
- *Ridistribuzione* dinamica delle risorse durante la completa scansione del sistema;
- *Firewall personale* con sistema di rilevamento intrusione e avviso circa gli attacchi alla rete;
- *Sicura operatività per gli utenti in qualsiasi* tipo di Network compreso Wi-Fi;
- *Protezione dagli attacchi phishing e junk mail;*
- *Capacità di disinfezione remota* (Intel® Active Management, Intel® vPro™);
- *Rollback per modifiche pericolose del sistema;*
- *Auto-Difesa da programmi maligni;*
- *Completo supporto per sistemi operativi a 64-bit;*
- *Aggiornamento automatico dei database.*

Kaspersky Security for Mail Servers

Questo programma è per proteggere i server di posta ed i server collegati da programmi pericolosi e da spam. Il programma comprende l'applicazione per proteggere tutti server di posta standard (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix ed Exim) e abilita a configurare un gateway e-mail dedicato. La soluzione include:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Le sue caratteristiche comprendono:

- Affidabile protezione contro programmi maligni o potenzialmente pericolosi;
- Filtro di junk mail;

- Scansione di tutti i messaggi ed si Microsoft Exchange Server per virus compreso le cartelle condivise;
- Controllo di e-mail, database ed altri oggetti per server Lotus Notes/Domino;
- Filtro delle e-mail per tipo di allegato;
- Oggetti sospetti in Quarantena;
- Semplice sistema di gestione del programma;
- Prevenzione epidemia virus;
- Monitoraggio stato protezione a mezzo notifiche;
- Sistema di reportistica per l'operatività del programma;
- Scalabilità del pacchetto software in accordo con la capacità delle risorse disponibili di sistema;
- Aggiornamento automatico dei database.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, i moderni metodi di filtro della posta elettronica (incluse le liste nere DNS e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, dove controlla le e-mail in arrivo dallo spam, Kaspersky® Anti-Spam funziona come barriera alle e-mail indesiderate. Il prodotto è compatibile con qualsiasi sistema di posta e può essere installato sia su server di posta esistente sia su server dedicati.

L'elevato grado di efficacia di Kaspersky Anti-Spam è consentito dall'aggiornamento quotidiano del database di filtro dei contenuti,con l'aggiunta di campioni forniti specialisti del laboratorio linguistico della Società. I database vengono aggiornati ogni 20 minuti.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® per MIMESweeper assicura una elevata velocità di scansione del traffico sui server funzionanti con Clearswift MIMEsweeper per SMTP / Clearswift MIMEsweeper per Exchange / Clearswift MIMEsweeper per Web.

Il programma è un plug-in e scansiona contro i virus e processa in tempo reale il traffico e-mail in ingresso ed in uscita.

B.2. Recapiti

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab. che sarà lieta di offrire assistenza per qualsiasi problematica relativa ai suoi prodotti, sia per telefono che per e-mail. Tutte le raccomandazioni e i suggerimenti pervenuti saranno presi in considerazione e valutati con attenzione.

Supporto tecnico	Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina: http://www.kaspersky.com/supportinter.html Helpdesk: http://support.kaspersky.ru/helpdesk.html?LANG=it
Informazioni generali	WWW: http://www.kaspersky.it http://www.viruslist.com Messaggio: info@kaspersky.com

APPENDICE C. CONTRATTO DI LICENZA

Contratto di licenza standard con l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: SI RACCOMANDA DI LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO DI LICENZA ("CONTRATTO"), PER LA LICENZA DEL SOFTWARE KASPERSKY INTERNET SECURITY ("SOFTWARE") PRODOTTO DA KASPERSKY LAB.

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO E A DIVENTARNE UNA DELLE PARTI. IN CASO CONTRARIO, FACENDO CLIC SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DI TUTTE LE CONDIZIONI DEL PRESENTE, L'UTENTE RINUNCIA A INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO SU SUPPORTO FISICO E L'UTENTE HA ROTTO IL SIGILLO DELLA BUSTA DEL CD, ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. SE L'UTENTE NON ACCETTA TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, EGLI DOVRÀ ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE.

AI SENSI DELLA LEGISLAZIONE VIGENTE, PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI, ACQUISTATO ONLINE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE HA QUATTORDICI (15) GIORNI LAVORATIVI DI TEMPO DALLA CONSEGNA DEL PRODOTTO PER RESTITUIRLO AL RIVENDITORE A FINI DI SOSTITUZIONE O DI RIMBORSO, A CONDIZIONE CHE IL SOFTWARE NON SIA STATO DISSIGILLATO.

PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI NON ACQUISTATO ONLINE VIA INTERNET, QUESTO SOFTWARE NON POTRÀ ESSERE RESTITUITO NÉ SOSTITUITO, ECCEZION FATTA PER LE CLAUSOLE CONTRARIE DEL PARTNER CHE VENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON SARÀ RITENUTO RESPONSABILE DELLE CLAUSOLE DEL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Qualsiasi riferimento al "Software" nel presente documento sarà da intendersi comprensivo di codice di attivazione fornito da Kaspersky Lab come parte integrante di Kaspersky Internet Security 7.0.

1. *Concessione della licenza.* Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione in accompagnamento (la "Documentazione") per la durata del presente Contratto e unicamente a uso aziendale interno. È possibile installare una copia del Software su un computer.

1.1 *Uso.* Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un computer o da più di un utente per volta, salvo diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (per esempio random access memory o RAM) oppure installato nella memoria permanente (per esempio disco fisso, CD-ROM o altro dispositivo di memorizzazione) di quel computer. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di archivio, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Il software protegge il computer dai virus le cui firme sono contenute nel database di descrizione delle minacce che è disponibile sui server di aggiornamento di Kaspersky Lab.

1.1.3. Se vendi il computer sul quale è installato il Software dovrai assicurare che tutte le copie del Software siano state precedentemente eliminate.

1.1.4 È fatto divieto all'utente di decompilare, reverse engineer, disassemblare o altrimenti ridurre qualsiasi parte di questo Software in forma umanamente leggibile o consentire a terzi di farlo. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi indipendenti per computer saranno fornite da Kaspersky Lab dietro richiesta e pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab ti notificasse che, per qualsiasi ragione, inclusi (senza limitazioni) i costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire solo le operazioni di decompilazione o reverse engineering nei limiti previsti dalla legge.

1.1.5 L'utente non deve né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente) di effettuare la correzione di errori o

altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.6 È fatto divieto all'utente di concedere in locazione, in leasing o in prestito a terzi il Software o trasferire o cedere in sublicenza a terzi i diritti a lui conferiti dalla licenza.

1.1.7 E' vietato all'utente fornire il codice di attivazione o la chiave di licenza a terze parti o permettere a terze parti l'accesso ai codici di attivazione o alla chiave della licenza. Il codice di attivazione e la chiave della licenza sono dati riservati.

1.1.8 Kaspersky Lab può richiedere all'utente di installare l'ultima versione del Software (l'ultima versione ed il più recente pack di manutenzione).

1.1.9 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati maligni.

2. *Assistenza.*

(i) Kaspersky Lab metterà a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito per un periodo, specificato nel File della Chiave di Licenza ed indicato nella finestra Servizio, dal momento dell'attivazione, previo:

(a) pagamento della tariffa di assistenza corrente, e;

(b) compilazione del Modulo di iscrizione ai Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale sarà richiesto all'utente di fornire il proprio codice di attivazione fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria assoluta discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.

Il servizio di assistenza diventerà disponibile in seguito all'attivazione del Software. Il servizio di assistenza tecnica di Kaspersky Lab ha facoltà di richiedere all'utente finale un'ulteriore registrazione per poter usufruire dei servizi di assistenza.

Fino all'attivazione del Software e/o all'ottenimento dell'identificativo dell'utente finale (ID cliente) il servizio di assistenza tecnica offre assistenza esclusivamente per l'attivazione del Software e la registrazione dell'utente finale.

(ii) Con la compilazione del Modulo di sottoscrizione ai servizi di assistenza, l'utente accetta i termini della politica di tutela della riservatezza adottata da Kaspersky Lab e consultabile su

www.kaspersky.com/privacy, e acconsente esplicitamente al trasferimento dei propri dati in paesi esterni a quello di residenza, come specificato nella politica di tutela della riservatezza.

(iii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza.

(iv) Per "Servizi di assistenza" si intendono:

(a) Aggiornamento del database antivirus ogni ora;

(b) Aggiornamento database degli attacchi al network;

(c) Aggiornamento del database anti-spam;

(d) Aggiornamenti gratuiti del software comprese le versioni di aggiornamento;

(e) Supporto Tecnico via Internet e linea telefonica dedicata da parte dei commercianti e rivenditori;

(f) Aggiornamenti per il rilevamento e l'eliminazione di virus entro 24 ore.

(v) I servizi di assistenza sono forniti solo se e quando l'utente dispone della versione del Software più recente (compresi i pacchetti di manutenzione) disponibile sul sito web ufficiale Kaspersky Lab (www.kaspersky.com) installata sul computer.

3. *Diritti di proprietà.* Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

4. *Riservatezza.* L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del codice di attivazione.

5. *Garanzia limitata.*

(i) Kaspersky Lab garantisce che per un periodo di [6] mesi a decorrere dal primo caricamento o installazione il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità relativamente al fatto che il presente Software soddisfi i propri requisiti. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.

(vi) Le garanzie e le condizioni stabilite dal presente Contratto sostituiscono eventuali altre condizioni, garanzie o termini relativi alla fornitura o fornitura presunta dello stesso; la mancata fornitura o eventuali ritardi nella fornitura del Software o della Documentazione che, salvo per il presente paragrafo (vi) potrebbero avere effetto tra Kaspersky Lab e l'utente o potrebbero essere diversamente impliciti o integrati nel presente Contratto o in un eventuale accordo collaterale mediante statuto, diritto consuetudinario o altrimenti, sono esclusi mediante il presente (inclusi, senza tuttavia ad essi limitarsi, le condizioni implicite, le garanzie o altri termini relativi a qualità soddisfacente, idoneità per l'uso previsto o esercizio di ragionevoli competenze e cautele).

6. *Limitazione della Responsabilità.*

(i) Nessun elemento del presente Contratto escluderà o limiterà la responsabilità di Kaspersky Lab per (a) falso e frode, (b) decesso o lesioni personali causate da un suo mancato esercizio di tutela ai sensi del diritto consuetudinario o dalla violazione negligente di una delle

clausole del presente Contratto, o (c) eventuali altre responsabilità che non possano essere escluse per legge.

(ii) Ai sensi del paragrafo (i) di cui sopra, Kaspersky Lab non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):

(a) perdita di reddito;

(b) perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);

(c) perdita di liquidità;

(d) perdita di risparmi presunti;

(e) perdita di affari;

(f) perdita di opportunità;

(g) perdita di avviamento;

(h) danni alla reputazione;

(i) perdita, danni o corruzione di dati; o :

(j) eventuali perdite o danni indiretti o conseguenti o danni in qualsiasi modo arrecati (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nei paragrafi (ii), da (a) a (ii), (i)).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

7. Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi, impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto.

Quando si utilizza il Software demo, l'utente non può usufruire del Servizio Tecnico specificato nella Clausola 2 di questo EULA e neppure ha diritto di vendere la copia in possesso a terze parti.

All'utente è concesso l'uso del software a scopi dimostrativi per il periodo riportato nel file della chiave di avvio dal momento dell'attivazione (questo periodo può essere visto nella finestra Servizio del GUI del software).