



IBM Security Trusteer Rapport

Podręcznik użytkownika

Wersja 3.5.1403

Grudzień 2014 r.

Uwagi

Niniejsza publikacja została opracowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych. IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przysyłać na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japonia

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z przepisami prawa miejscowego:

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE "AS IS" BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŻNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy typograficzne. Informacje te są okresowo aktualizowane, a zmiany te zostaną uwzględnione w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych podmiotów zostały wprowadzone wyłącznie dla wygody użytkownika i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjodawcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Corporation
224A/101
11400 Burnet Road
Austin, TX 78758 USA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, zostanie uiszczona stosowna opłata.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły być dokonywane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów innych niż produkty IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. IBM nie testował tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów innych podmiotów należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są propozycjami cen detalicznych. Ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Wszelkie podane tu informacje mogą zostać zmienione, zanim opisywane produkty staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennej pracy. W celu kompleksowego ich zilustrowania podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiegokolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

Licencja w zakresie praw autorskich

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności i funkcjonalności tych programów. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym IBM.

Każda kopia programu przykładowego lub jakiegokolwiek jego fragment, jak też jakiegokolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika, rok). Fragmenty niniejszego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. 2004, 2014. Wszelkie prawa zastrzeżone.

W przypadku przeglądania niniejszych informacji w formie elektronicznej zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Znaki towarowe

IBM, logo IBM oraz ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corp. zarejestrowanymi w wielu systemach prawnych na całym świecie. Nazwy innych produktów i usług mogą być znakami towarowymi IBM lub innych podmiotów. Aktualna lista znaków towarowych IBM jest dostępna w serwisie WWW, w sekcji "Copyright and trademark information" (Informacje o prawach autorskich i znakach towarowych), pod adresem www.ibm.com/legal/copytrade.shtml.



Adobe, Acrobat, PostScript oraz wszystkie pochodne znaki towarowe są zastrzeżonymi znakami towarowymi lub znakami towarowymi Adobe Systems Incorporated w Stanach Zjednoczonych i w innych krajach.

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.



Java oraz wszystkie znaki towarowe i logo dotyczące języka Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Postanowienia dotyczące ochrony prywatności

Oprogramowanie IBM, w tym rozwiązanie SaaS (Software as a Service), zwane dalej "Oferowanym Oprogramowaniem" może korzystać z informacji cookie lub z innych technologii do gromadzenia danych o używaniu produktów, do poprawienia jakości usług dla użytkowników końcowych, do dopasowania interakcji do ich oczekiwań oraz do innych celów. W wielu przypadkach Oferowane Oprogramowanie nie gromadzi informacji pozwalających na identyfikację osoby.

Więcej informacji na temat korzystania z różnych technologii, w tym z informacji cookie, do opisanych wyżej celów znajduje się w sekcji "IBM Software Products and Software-as-a-Service Privacy Statement" pod adresem <http://www.ibm.com/software/info/product-privacy>.

Spis treści

Uwagi	ii
Licencja w zakresie praw autorskich	iii
Znaki towarowe	iii
Postanowienia dotyczące ochrony prywatności	iv
1. Informacje wstępne	1
O tym podręczniku	1
<i>Więcej informacji na temat programu Rapport</i>	1
<i>Przesyłanie opinii</i>	1
Informacje o wsparciu	2
Ułatwienia dostępu	2
Sprawdzone procedury w zakresie bezpieczeństwa	3
2. Czym jest program Rapport?	4
Oprogramowanie antywirusowe: fałszywe poczucie bezpieczeństwa	5
Wykrywanie podpisów nie działa	6
Strategia działania programu Rapport	6
Dodatkowa warstwa zabezpieczeń	7
Jak działa program Rapport	7
Sprawdzona technologia IBM	8
Obsługa	8
Dodatkowe funkcje programu Rapport	9
3. Instalowanie programu Rapport	10

Instalowanie programu Rapport w systemie operacyjnym Windows 8 za pośrednictwem przeglądarki Internet Explorer	13
Instalowanie programu Rapport w systemie operacyjnym Windows Server (2003 i 2008)	17
Jak mogę przełączyć się na konto administratora?	18
4. Pierwsze kroki	19
Otwórz Konsolę Rapport	20
5. Reagowanie na alerty i ostrzeżenia	22
Reagowanie na oferty ochrony hasła	22
Reagowanie na ostrzeżenia dotyczące danych chronionych	27
Reagowanie na ostrzeżenia dotyczące wprowadzania danych bez zabezpieczenia	29
Reagowanie na ostrzeżenia dotyczące wyludzania informacji	31
Reagowanie na ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej	33
Reagowanie na komunikaty o ochronie karty płatniczej	35
Reagowanie na alerty o wykryciu próby wykonania zrzutu ekranu	36
Reagowanie na alerty dotyczące ochrony przeglądarki	37
Reagowanie na alerty dotyczące aktywacji funkcji usuwania szkodliwego oprogramowania	38
Reagowanie na alerty dotyczące zainicjowania usuwania szkodliwego oprogramowania	40
Reagowanie na ostrzeżenia dotyczące niepoprawnego certyfikatu	41
Reagowanie na standardowe ostrzeżenia dotyczące konta użytkownika	44
Reagowanie na powiadomienia dotyczące raportu o aktywności	45
Reagowanie na komunikaty o potwierdzeniu aktualizacji kodu	45

Reagowanie na ostrzeżenia dotyczące trybu zgodności z lektorem ekranowym	46
Reagowanie na alerty dotyczące ponownej instalacji w trybie administratora	47
<i>Przełączanie się na konto administratora (system operacyjny Windows 8)</i>	49
<i>Przełączanie się na konto administratora (system operacyjny Windows 7)</i>	50
<i>Przełączanie się na konto administratora (system operacyjny Windows XP)</i>	52
6. Dostosowywanie programu Rapport	54
Ukrywanie i przywracanie ikony programu Rapport na pasku adresu	54
Ukrywanie i przywracanie ikony na pasku zadań	55
Zmiana języka interfejsu	56
7. Wyświetlanie informacji o aktywności programu Rapport	57
Wyświetlanie raportu o aktywności	57
Konfigurowanie raportu o aktywności	58
<i>Czyszczenie raportu o aktywności</i>	59
<i>Wyłączanie raportu o aktywności</i>	59
8. Zarządzanie chronionymi serwisami i hasłami	60
Ochrona dodatkowych serwisów WWW	61
Usuwanie chronionych serwisów WWW	63
Zarządzanie chronionymi nazwami użytkowników i hasłami	64
9. Rozwiązywanie problemów	66
Zatrzymywanie programu Rapport	66
Uruchamianie programu Rapport	67
Uzyskiwanie wsparcia	68

Odblokowywanie uprawnionych programów dodatkowych przeglądarki	69
Wyłączanie blokady rejestrowania naciśnień klawiszy	70
Cofanie przypadkowych autoryzacji	71
<i>Usuwanie autoryzowanych nieważnych certyfikatów SSL</i>	72
<i>Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych kart płatniczych</i>	73
<i>Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych bez zabezpieczenia</i>	74
<i>Usuwanie serwisów WWW, dla których zezwolono na wysyłanie danych logowania</i>	76
Postępowanie w przypadku błędów	77
<i>Postępowanie w przypadku błędów aktualizacji</i>	77
<i>Postępowanie w przypadku błędów instalatora programu Rapport</i>	78
<i>Postępowanie w przypadku błędów dotyczących deinstalacji</i>	79
Konfigurowanie serwera proxy na potrzeby automatycznych aktualizacji	80
Wysyłanie przez użytkownika raportu o problemie	81
Kopiowanie identyfikatora programu Trusteer Endpoint Protection	82
Wysyłanie plików dzienników programu Rapport do IBM	82
10. Aktualizowanie programu Rapport	83
Sprawdzanie statusu aktualizacji programu Rapport	83
Ręczne aktualizowanie programu Rapport	85
Wyłączanie automatycznych aktualizacji	87
11. Deinstalowanie programu Rapport	89
Deinstalowanie programu Rapport (Windows 8 i Windows 7)	90
Deinstalowanie programu Rapport (Windows XP)	90

1. Informacje wstępne

O tym podręczniku

W tym podręczniku wyjaśniono sposób korzystania z programu IBM Security Trusteer Rapport ("Rapport") w sposób zapewniający optymalne wykorzystanie jego możliwości. Podręcznik jest przeznaczony dla:

- klientów banków i innych instytucji finansowych, oferujących program Rapport do bezpłatnego pobrania jako narzędzie chroniące rachunki bankowe obsługiwane za pośrednictwem Internetu;
- klientów korzystających z kart płatniczych chronionych przez program Rapport, korzystających z programu Rapport do zabezpieczenia transakcji realizowanych online za pomocą kart płatniczych.

Więcej informacji na temat programu Rapport

Jako uzupełnienie tego podręcznika dostępna jest opracowana przez IBM strona <http://www.trusteer.com/support/faq>, zawierająca często zadawane pytania.

Na stronie WWW zawierającej często zadawane pytania należy wprowadzić swoje pytanie w narzędziu Błyskawiczne odpowiedzi w celu uzyskania odpowiedzi na dodatkowe, mogące się pojawić pytania i wątpliwości.

Przesyłanie opinii

Opinie użytkowników są dla IBM bardzo ważne.

- Zachęcamy do przesyłania sugestii dotyczących nowych funkcji oraz udoskonaleń i wyrażania swoich opinii na temat programu Rapport.

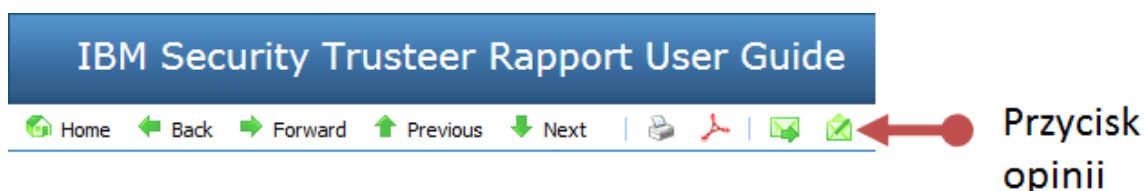
W celu przesłania opinii na temat programu Rapport należy przejść pod adres:

<http://www.trusteer.com/support/product-feedback>.

- Zachęcamy do przesyłania sugestii dotyczących nowych tematów oraz udoskonaleń i wyrażania swoich opinii na temat niniejszego Podręcznika użytkownika.

➔ **Aby przesłać opinię o Podręczniku użytkownika:**

Kliknij przycisk przesyłania opinii  u góry strony Podręcznika użytkownika programu Rapport. Przycisk ten powoduje otwarcie strony, za pośrednictwem której można przesłać opinię.



Informacje o wsparciu

Informacje na temat wsparcia są dostępne w serwisie:

<http://www.trusteer.com/support>

Ułatwienia dostępu

Ułatwienia dostępu pomagają użytkownikom niepełnosprawnym, np. osobom z upośledzoną motoryką lub niedowidzącym, w efektywnym korzystaniu z oprogramowania. Opiswany tutaj produkt oferuje ułatwienia dostępu polegające na możliwości nawigacji w interfejsie na podstawie informacji odczytywanych na głos przez program.

Sprawdzone procedury w zakresie bezpieczeństwa

Bezpieczeństwo systemów informatycznych wymaga ochrony systemów i informacji poprzez działania prewencyjne, wykrywanie zagrożeń i reagowanie w przypadku niewłaściwego dostępu w obrębie organizacji i poza nią. Niewłaściwy dostęp może spowodować zmiany w informacjach, ich zniszczenie, wykorzystanie w niewłaściwy sposób albo też uszkodzenie systemu lub niewłaściwe wykorzystanie systemów, w tym użycie ich do zaatakowania innych systemów. Żaden system ani produkt informatyczny nie jest całkowicie bezpieczny. Żaden pojedynczy produkt, usługa czy zabezpieczenie nie gwarantują pełnej skuteczności ochrony przed niewłaściwym użyciem lub dostępem. Systemy, produkty i usługi IBM® zostały zaprojektowane jako część kompleksowego rozwiązania w zakresie zabezpieczeń, obejmującego niezbędne dodatkowe procedury operacyjne i mogącego wymagać większej skuteczności innych systemów, produktów czy usług. IBM NIE GWARANTUJE, ŻE SYSTEMY, PRODUKTY CZY USŁUGI SĄ ODPORNE NA DZIAŁANIA PODEJMOWANE PRZEZ OSOBY TRZECIE W ZŁEJ WIERZE LUB BEZPRAWNIE ANI ŻE TAKIE SYSTEMY, PRODUKTY CZY USŁUGI ZABEZPIECZĄ ORGANIZACJĘ PRZED TAKIMI DZIAŁANIAM I OSÓB TRZECICH.

2. Czym jest program Rapport?

Rapport to zaawansowane oprogramowanie zabezpieczające opracowane z myślą o zapobieganiu kradzieży danych bankowych przekazywanych drogą elektroniczną. Program Rapport jest polecany i oferowany przez Państwa bank jako dodatkowa warstwa ochrony, w uzupełnieniu oprogramowania antywirusowego lub zabezpieczającego, z którego być może już Państwo korzystają. Chroniąc połączenie z Internetem i tworząc kanał bezpiecznej komunikacji z serwisem WWW banku, program Rapport blokuje próby kradzieży środków pieniężnych z rachunku bankowego.

Krótki film wideo o charakterze wprowadzającym do programu Rapport można znaleźć pod adresem <http://www.trusteer.com/introduction-to-rapport>

Z korzystania z programu Rapport nie należy rezygnować nawet w sytuacji, w której komputer i sieć są chronione za pomocą innych rozwiązań do ochrony komputera i komunikacji sieciowej. Ostatnie badania wskazują, że rozwiązania z zakresu zabezpieczeń, takie jak oprogramowanie antywirusowe czy firewall, charakteryzują się tylko częściową skutecznością wobec wymierzonych w serwisy finansowe ataków szkodliwego oprogramowania takiego jak Zeus, SpyEye, Gozi czy Torpig. Dzięki integracji z procesami zapobiegania władowaniom oferowanymi przez bank program Rapport gwarantuje dodatkową warstwę zabezpieczeń, obok innych rozwiązań do ochrony komputera i komunikacji sieciowej. Program Rapport umożliwia wykrywanie najbardziej wyrafinowanych ataków o charakterze finansowym, wyświetlanie informujących o nich alertów i blokowanie takich ataków.

Program Rapport jest udostępniany użytkownikom bezpłatnie i umożliwia ochronę sesji bankowości elektronicznej oraz innych serwisów WWW niezwiązanych z bankiem, takich jak sklepy internetowe lub serwisy poczty elektronicznej.

Na ile rozpowszechnione są cyberprzestępstwa o charakterze finansowym?

W roku 2011 FBI zidentyfikowało dwadzieścia incydentów polegających na oszustwach na łączną sumę 20 mln USD, polegających na kradzieży danych uwierzytelniających do bankowości elektronicznej małej i średniej wielkości przedsiębiorstw amerykańskich i użyciu ich do zainicjowania przelewów bankowych do chińskich przedsiębiorstw z sektora handlowego. Według szacunków cyberprzestępcy okradają małe i średnie przedsiębiorstwa w Stanach Zjednoczonych i Europie na kwotę nawet 1 mld USD rocznie. Korporacyjne rachunki bankowe to szczególnie narażone na ataki cyberprzestępców cele, a liczba takich ataków stale rośnie. Jedno z największych zagrożeń wiąże się z komputerem wykorzystywanym do wykonywania operacji bankowych. Przestępcy wykorzystują dwie wyrafinowane metody dostępu do rachunków online za pośrednictwem komputera:

- **Szkodliwe oprogramowanie** — automatycznie i bez wiedzy użytkownika pobierane na jego komputer podczas korzystania z Internetu przechwytuje dane logowania i przesyła je do grupy przestępczej, a także umożliwia modyfikację bez wiedzy użytkownika realizowanych transakcji.
- **Wyludzanie informacji** — przestępcy budują fałszywe serwisy WWW łudząco przypominające serwis WWW banku, aby skłonić użytkownika do wprowadzenia w nich danych logowania do bankowości elektronicznej, które zostaną następnie użyte do uzyskania dostępu do rachunku bankowego.

Oprogramowanie antywirusowe: fałszywe poczucie bezpieczeństwa

Jest taka rzecz, którą producenci oprogramowania antywirusowego woleliby przed Tobą ukryć: oferowane przez nich produkty nie są szczególnie skuteczne w zakresie blokowania najbardziej wyrafinowanych wirusów. Jak podaje serwis Krebs On Security, statystyki wskazują, że **oprogramowanie antywirusowe wykrywa zaledwie około 25% najbardziej popularnego szkodliwego oprogramowania** przesyłanego obecnie za pośrednictwem poczty e-mail. Dzieje się tak, ponieważ twórcy wirusów działają bardzo szybko. Zwykle w chwili, gdy oprogramowanie antywirusowe potrafi

wykryć daną, nową odmianę wirusa, jest już za późno. Jest to moment, gdy cyberprzestępcy zdobyli już dostęp do rachunków bankowych klientów.

Wykrywanie podpisów nie działa

W celu zidentyfikowania nowych wirusów (zwanych również „szkodliwym oprogramowaniem”) rozwiązania antywirusowe tworzą specjalne sygnatury każdego przychodzącego pliku, a następnie porównują je ze słownikiem sygnatur znanych wirusów. Rozwiązania antywirusowe nie mogą bronić się przed szkodliwym oprogramowaniem, o ile wcześniej nie została pozyskana próbka pliku i nie zostanie opracowana sygnatura.

Problem polega na tym, że autorzy szkodliwego oprogramowania są także bardzo, bardzo przebiegli. Są oni w stanie stworzyć miliony plików — każdy z unikatowym podpisem — miesięcznie. To samo szkodliwe oprogramowanie może być maskowane w wielu różnych plikach, przy czym każdy powinien mieć własny podpis nieznany oprogramowaniu antywirusowemu.

Wykrycie nowych podpisów przez szkodliwe oprogramowanie służące do przestępstw finansowych przez programy antywirusowe może zająć wiele dni, a nawet tygodni. Jednocześnie wyłudzenie może mieć miejsce w ciągu zaledwie godzin po powstaniu nowego szkodliwego oprogramowania o nieznanym dotąd podpisie. Tak więc w chwili, gdy dostawca oprogramowania antywirusowego oczyści komputer ze szkodliwego oprogramowania, może być już za późno na zapobieżenie wyłudzeniu.

Strategia działania programu Rapport

Innowacyjna technologia IBM wkracza tam, gdzie zawodzi tradycyjne oprogramowanie zabezpieczające. Od momentu zainstalowania programu Rapport chroni urządzenie użytkownika i łagodzi ryzyko związane z zainfekowaniem go przez szkodliwe oprogramowanie finansowe. IBM komunikuje się z bankiem, umożliwiając jego specjalistom natychmiastowe reagowanie na nowe zagrożenia.

Program Rapport nie umożliwia wyszukiwania podpisów plików. Nie sprawdza on też samego pliku, ale jego aktywność. Program Rapport wykrywa proces instalacji szkodliwego oprogramowania i przerywa go, chroniąc komputer przed infekcją. Nawet w sytuacji, gdy dojdzie do instalacji szkodliwego oprogramowania na urządzeniu, program Rapport wykrywa i blokuje próby naruszenia ochrony przeglądarki oraz sesji bankowości elektronicznej. Blokując działalność szkodliwego oprogramowania, program Rapport zapewnia ochronę na poziomie uzupełniającym i przewyższającym możliwości programów antywirusowych. To właśnie dlatego Państwa bank podjął współpracę z IBM — aby zapewnić sobie oraz swoim klientom najlepszą ochronę przed oszustwami finansowymi.

Dodatkowa warstwa zabezpieczeń

Program Rapport zoptymalizowano pod kątem blokowania szkodliwego oprogramowania i nadużyć finansowych. Nie oznacza to jednak, że należy całkowicie zrezygnować z posiadanych rozwiązań antywirusowych. Wiele innych wirusów nadal stanowi zagrożenie. Mogą one spowalniać pracę komputera lub zakłócać pracę, nie będą natomiast podejmowały prób wyłudzenia środków finansowych. Należy nadal stosować rozwiązania antywirusowe posiadane przez użytkownika do ochrony przed wirusami tego typu.

Jak działa program Rapport

- Natychmiast usuwa szkodliwe oprogramowanie z komputera.
- Zapobiega infekcjom szkodliwym oprogramowaniem po wejściu na szkodliwe strony lub pobraniu szkodliwych aplikacji.
- Blokuje ataki mające na celu wyłudzenie danych uwierzytelniających oraz innych informacji.
- Automatycznie pobiera aktualizacje w tle, zapewniając ochronę przed nowymi zagrożeniami.
- Jest „lekkim” oprogramowaniem, które nie spowalnia pracy komputera ani nie zakłóca pracy aplikacji.

- Ochrona rozpoczyna się już z chwilą zakończenia szybkiej instalacji (aby zapewnić pełną ochronę, należy zrestartować komputer).

Sprawdzona technologia IBM

Program Rapport został opracowany przez specjalistów IBM ds. bezpieczeństwa internetowego. Obecnie oprogramowanie to zapewnia ochronę dziesiątkom milionów użytkowników na całym świecie. W niezależnym badaniu Rapport powstrzymał 100% szkodliwych programów, którymi testerzy próbowali zainfekować chroniony komputer.

Obsługa

Program Rapport jest prosty w obsłudze. Korzystanie z niego nie wymaga dysponowania wiedzą techniczną. Program Rapport nie wymaga także przeprowadzenia dodatkowych czynności konfiguracyjnych, nie zmienia sposobu pracy użytkownika, nie powoduje modyfikacji sposobu działania przeglądarki i nie wyświetla po napotkaniu zagrożenia pytań o charakterze technicznym.

Większość z operacji realizowanych przez program Rapport jest realizowana w tle i nie zakłóca pracy użytkownika ani nie wymaga jego udziału. Program Rapport rejestruje wszystkie czynności podejmowane w celu ochrony użytkownika w [raporcie o aktywności](#), którego wyświetlenie jest możliwe w dowolnej wybranej przez niego chwili. Szczegółowe informacje na temat poziomów ryzyka można znaleźć w raporcie o aktywności. Po napotkaniu przez program Rapport poważnego zagrożenia powiadamia on o tym fakcie użytkownika. Niektóre podejmowane w takich przypadkach czynności wymagają prostego reagowania na [Ostrzeżenia programu Rapport](#), które są szczególnie łatwe do zrozumienia.

Sprawdzenie, które serwisy WWW są chronione przez program Rapport, nie następuje wielu trudności. Po prawej stronie paska adresu przeglądarki (lub w pobliżu) wyświetlana jest ikona, której kolor wskazuje, czy aktualnie odwiedzany serwis jest chroniony.



Ikona program Rapport () pojawia się na pasku zadań systemu Windows, jeśli program Rapport jest uruchamiany. Kliknięcie ikony na pasku zadań powoduje otwarcie Konsoli Rapport, za pośrednictwem której można uzyskać dostęp do różnych funkcji i informacji programu Rapport.

Przy każdym użyciu nowych danych logowania w chronionym serwisie program Rapport wyświetla okno dialogowe z ofertą [ochrony tych danych uwierzytelniających](#). To okno dialogowe pojawia się tylko przy pierwszym użyciu danych logowania.

Dodatkowe funkcje programu Rapport

Obok ochrony uzyskiwanej automatycznie przy nawiązywaniu połączenia z serwisami WWW partnerów IBM możliwe jest ręczne dodanie zabezpieczeń programu Rapport do wszystkich pozostałych używanych serwisów WWW. Więcej informacji można znaleźć w punkcie [Ochrona dodatkowych serwisów WWW](#).

Rapport może również generować [raporty](#) na temat prób włamania na konto bankowości elektronicznej użytkownika.

3. Instalowanie programu Rapport

Instalowanie programu Rapport jest szybkie i proste. Wystarczy pobrać plik instalacyjny ze strony WWW banku, uruchomić go i postępować zgodnie ze wskazówkami w standardowym kreatorze instalacji.

Dalsze instrukcje można znaleźć w punkcie [Instalowanie programu Rapport w systemie Windows 8 za pośrednictwem przeglądarki Internet Explorer](#). Instrukcje dotyczące instalowania programu Rapport w innych przeglądarkach WWW można znaleźć na stronie WWW:

<http://www.trusteer.com/support/win-install-instructions>.

Jeśli program Rapport jest instalowany za pośrednictwem konta administratora systemu Windows, standardowy użytkownik może uruchomić program Rapport ze swojego konta, ale nie może zatrzymać ani rozpocząć procesu instalacji, zdeinstalować ani ponownie zainstalować programu Rapport, ani nie może zmieniać ustalonych ustawień strategii. Ograniczenie to umożliwia administratorom instalowanie programu Rapport na urządzeniach całego przedsiębiorstwa, jednocześnie uniemożliwiając wyłączanie opcji zabezpieczających przez pracowników lub modyfikowanie przez nich strategii bezpieczeństwa dotyczących wszystkich użytkowników.

Zdecydowanie zaleca się instalację programu Rapport z konta administratora, ponieważ powoduje to automatyczne rozszerzenie ochrony na wszystkich użytkowników. Ponadto nie jest możliwe instalowanie sterowników w przypadku instalowania programu Rapport ze standardowego konta użytkownika, zaś najważniejsze mechanizmy zabezpieczające programu Rapport (ochrona przed szkodliwym programowaniem i deinstalowanie go) są instalowane za pośrednictwem sterowników.

W przypadku instalowania programu Rapport ze standardowego konta użytkownika nie będzie on mógł być uruchamiany z żadnego innego konta użytkownika, a jego instalacja nie będzie możliwa na żadnym innym koncie, o ile nie zostanie on najpierw zdeinstalowany.

Skąd można pobrać program Rapport?

Będąc klientem banku lub innej organizacji oferującej program Rapport, można pobrać go ze strony WWW banku. Bank może:

- Wyświetlić sekcję zabezpieczeń na stronie WWW banku (zwykle w dolnej części strony) wraz z odsyłaczem do programu Rapport lub odsyłaczem do strony umożliwiającej pobranie oprogramowania zabezpieczającego.
- Zaoferować możliwość pobrania programu Rapport w ramach procesu logowania do konta bankowości elektronicznej lub tuż po pomyślnym zalogowaniu.

Czy program Rapport działa z moim systemem operacyjnym i przeglądarką?

Program Rapport działa z następującymi systemami operacyjnymi i przeglądarkami:
<http://www.trusteer.com/supported-platforms>.

Dlaczego otrzymuję komunikat informujący, że program Rapport już istnieje na moim komputerze?

Jeśli wersja programu Rapport już istnieje na komputerze podczas instalowania go, w procesie instalacji wyświetlane jest następujące okno dialogowe:



Wyświetlenie tego ekranu podczas instalacji oznacza, że na komputerze jest już zainstalowany program Rapport. Ponowna instalacja programu Rapport jest całkowicie bezpieczna (wystarczy upewnić się, że nie będzie instalowana wersja starsza, niż zainstalowana obecnie).

➔ **Aby zainstalować program Rapport zamiast już istniejącej wersji:**

1. Wybierz opcję najlepiej wyjaśniającą przyczynę zamiaru ponownej instalacji programu Rapport.
2. Kliknij opcję **Dalej**. Proces instalacji zostanie rozpoczęty, a następnie przerwany w celu zamknięcia programu Rapport. Przed zamknięciem programu Rapport zostanie wyświetlony komunikat z prośbą o wprowadzenie kodu zabezpieczającego. Do komunikatu dołączony jest obrazek ze słowem, które należy wpisać, aby uniemożliwić wyłączenie programu Rapport przez szkodliwe oprogramowanie.
3. Wprowadź znaki widoczne na obrazku. (Nie jest rozróżniana wielkość liter).
4. Kliknij opcję **Zamknij**. Podczas zamykania programu Rapport wyświetlany jest następujący komunikat: „Należy poczekać na zamknięcie programu Trusteer Endpoint Protection”. Zniknięcie tego komunikatu oznacza, że działanie programu Rapport zostało zatrzymane. Proces instalacji jest kontynuowany bez przeszkód. Po zakończeniu instalacji może zostać wyświetlony ekran z następującym komunikatem:

Nastąpiła aktualizacja programu Trusteer Endpoint Protection do nowej wersji. Niektóre nowe funkcje programu Trusteer Endpoint Protection będą dostępne dopiero po ponownym uruchomieniu.

Mimo wyświetlenia tego komunikatu komputer jest chroniony. Zaleca się jednak ponowne uruchomienie komputera tak szybko, jak to tylko możliwe.

W jaki sposób mogę zainstalować program Rapport w współużytkowanym środowisku pulpitu wirtualnego?

W przypadku instalowania programu Rapport w systemie operacyjnym Windows Server (2003 lub 2008) kreator instalacji wykrywa system operacyjny i instaluje wersję serwerową programu Rapport. Wersja ta obsługuje wiele sesji. Więcej informacji można znaleźć w punkcie [Instalowanie programu Rapport w systemie operacyjnym Windows Server \(2003 lub 2008\)](#).

Uwaga: Poniższa procedura opisuje instalację, w której program Rapport wdrożono w celu wymuszenia instalacji wersji administracyjnych. Więcej informacji na temat pozostałych opcji wdrożenia programu Rapport zawiera publikacja *Installing IBM Security Trusteer Rapport from a Standard User Account Best Practices*.

Instalowanie programu Rapport w systemie operacyjnym Windows 8 za pośrednictwem przeglądarki Internet Explorer

Ta procedura wyjaśnia sposób pobierania i instalowania programu Rapport w przypadku uruchamiania systemu operacyjnego Windows 8 i korzystania z przeglądarki Microsoft Internet Explorer. W przypadku innych przeglądarek stosowne instrukcje można znaleźć na stronie WWW:

<http://www.trusteer.com/support/win-install-instructions>.

➔ Aby zainstalować program Rapport:

1. Przejdź na stronę logowania swojej organizacji. Jeśli organizacja ta oferuje program Rapport do pobrania, zostanie wyświetlony ekran powitalny z przyciskiem **Pobierz teraz**.
2. Kliknij opcję **Pobierz teraz**. W dolnej części okna przeglądarki zostanie wyświetlony pasek informacyjny z pytaniem, czy plik RapportSetup.exe ma zostać uruchomiony, czy zapisany.
3. Kliknij opcję **Uruchom**. Kilka sekund później zostanie wyświetlone kolejne okno dialogowe z pytaniem: „Czy chcesz zezwolić następującemu programowi na wprowadzenie zmian na tym komputerze?”

4. Kliknij opcję **Tak**. Może zostać wyświetlone okno dialogowe z następującym komunikatem:

Próbujesz zainstalować program Trusteer Endpoint Protection, korzystając ze standardowego konta użytkownika systemu Windows. Przeprowadzenie instalacji z użyciem konta tego rodzaju nie pozwala na wykorzystanie zaawansowanych funkcji usuwania szkodliwego oprogramowania, dostępnych w produkcie Trusteer Endpoint Protection, i może spowodować wystawienie komputera na ryzyko. Z tego względu instalację należy przeprowadzić z użyciem uprawnień administratora.

Aby skorzystać z uprawnień administratora w systemie Windows i kontynuować proces instalacji, należy kliknąć przycisk Instaluj.

Jeśli komputer należy do firmy lub organizacji, może okazać się konieczny kontakt z jej działem IT.

Ten komunikat oznacza, że użytkownik jest obecnie zalogowany za pośrednictwem standardowego konta systemu Windows. IBM zaleca instalowanie programu Rapport za pośrednictwem konta administratora.

5. Kliknij opcję **Instaluj**. Zostanie wyświetlony monit z prośbą o wprowadzenie hasła administratora.

Uwaga: Jeśli nie możesz zainstalować programu Rapport z wykorzystaniem uprawnień administratora, możesz zamknąć to okno dialogowe. Nie zostanie wyświetlony monit o wprowadzenie hasła administratora, a instalator zostanie zamknięty.

6. Wprowadź hasło i kliknij przycisk **Tak**, aby kontynuować. Może zostać wyświetlone okno dialogowe z następującym komunikatem:

W związku z niniejszą instalacją mogą zostać wyświetlone okna dialogowe firewalla i oprogramowania antywirusowego z ostrzeżeniami związanymi z niniejszą instalacją.

Należy zezwolić programom RapportSetup lub RapportService na kontynuowanie pracy w przypadku wyświetlenia dowolnego z tych ostrzeżeń, wybierając opcję taką jak:

- Wyłącz blokadę
- Tak
- Zezwól
- Zezwalaj

Jeśli instalacja nie powiedzie się, może okazać się potrzebne czasowe wyłączenie oprogramowania antywirusowego lub zabezpieczającego i ponowienie próby instalacji. W przeciwnym wypadku oprogramowanie antywirusowe lub firewall — szczególnie w przypadku ustawienia wysokiego poziomu ochrony — mogą uniemożliwić poprawne zakończenie procesu instalacji.

7. Kliknij przycisk **OK**. Rozpocznie się pobieranie programu Rapport.

Zostanie wyświetlony kreator instalacji programu Trusteer Endpoint Protection Installation.

8. Jeśli chcesz, aby program Rapport był kompatybilny z lektorem ekranowym, kliknij opcję **Zaawansowane**. Zostanie wyświetlony ekran Opcje zaawansowane. Zaznacz opcję **Niedowidzę, mam problemy z rozróżnianiem kolorów i/lub korzystam z pomocy lektorów ekranowych**, a następnie kliknij przycisk **Kontynuuj**. Ten tryb umożliwia odczytywanie przez lektora ekranowego treści menu i okien dialogowych programu Rapport i eliminuje możliwość zablokowania działania lektora ekranowego przez program Rapport w oknie przeglądarki. Powoduje to także wyłączenie okien dialogowych z

zabezpieczeniami w postaci obrazka wyświetlanych przy zatrzymywaniu lub deinstalacji programu Rapport.

Uwaga: Nie należy zaznaczać pola wyboru **Niedowidzę, mam problemy z rozróżnianiem kolorów i/lub korzystam z pomocy lektorów ekranowych**, instalując program Rapport na komputerze nieprzeznaczonym dla osób korzystających z lektora ekranowego. Ustawienie to powoduje bowiem dezaktywację niektórych funkcji zabezpieczeń.

9. Kliknij opcję **Akceptuję warunki zawarte w umowie licencyjnej**.
10. Kliknij przycisk **Instaluj**. Proces instalacji będzie kontynuowany. Po zakończeniu procesu instalacji w kreatorze zostanie wyświetlony przycisk **Zakończ**.
11. Kliknij przycisk **Zakończ**. Po upływie kilku sekund program Rapport otwiera nowe okno przeglądarki umożliwiające wykonanie krótkiego testu kompatybilności. Po zakończeniu testu program Rapport otwiera stronę w przeglądarce użytkownika.

Proces instalacji jest zakończony.

Instalowanie programu Rapport w systemie operacyjnym Windows Server (2003 i 2008)

Program Rapport obsługuje system operacyjny Windows Server (2003 i 2008). Program Rapport obsługuje także wiele sesji użytkownika, umożliwiając obsługę wielu profili w jednej instalacji, tak jak jest to wymagane na potrzeby współużytkowanej infrastruktury pulpitu wirtualnego. Program Rapport wykrywa fakt uruchomienia procesu instalacji na serwerze Windows Server (2003 lub 2008) i instaluje wersję serwera uwzględniającą możliwość wyłączenia wysyłania komend ponownego uruchomienia do użytkowników. Wyłączenie możliwości wysyłania komend ponownego uruchomienia do użytkowników pomaga uniknąć sytuacji, w których jeden użytkownik restartuje system dla wszystkich użytkowników na danym komputerze. Informacje na temat wyłączania możliwości wydawania komend ponownego uruchomienia można znaleźć w publikacji *IBM Security Trusteer Rapport Virtual Environment Best Practices*.

➔ Aby zainstalować program Rapport w systemie operacyjnym Windows Server 2003 lub 2008:

1. Uruchom plik RapportSetup.exe. Plik ten można pobrać ze strony:
<http://www.trusteer.com/support/rapport-installation-links>.
2. Kontynuuj proces instalacji, umożliwiający pobranie kompletnego pakietu instalacyjnego oraz inicjalizację kreatora instalacji. Kreator instalacji wykrywa system operacyjny na serwerze i wyświetla ekran **Wykryto hosta w systemie operacyjnym Windows Server**.
3. Po wyświetleniu tego ekranu kliknij opcję **Wyświetl dokument**. W przeglądarce WWW otwierana jest [strona wsparcia dla przedsiębiorstw dotycząca programu Rapport](#), zawierająca wyjaśnienie sposobu, w jaki program Rapport pomaga chronić przedsiębiorstwa. Na stronie wsparcia firmy kliknij odsyłacz, aby wyświetlić dokument *IBM Security Trusteer Rapport Virtual Implementation Scenarios*, który udostępnia ważne informacje dotyczące implementacji programu Rapport w środowisku pulpitu wirtualnego.

4. Po zapoznaniu się z treścią dokumentu zaznacz pole wyboru **Potwierdzam zapoznanie się z dokumentem** i kontynuuj proces instalacji.

Inaczej, niż w przypadku ekranu **Wykryto hosta systemu Windows Server**, instalacja przebiega podobnie do instalacji w pozostałych systemach operacyjnych.

Jak mogę przełączyć się na konto administratora?

- [Przełączanie się na konto administratora \(system operacyjny Windows 8\)](#)
- [Przełączanie się na konto administratora \(system operacyjny Windows 7\)](#)
- [Przełączanie się na konto administratora \(system operacyjny Windows XP\)](#)

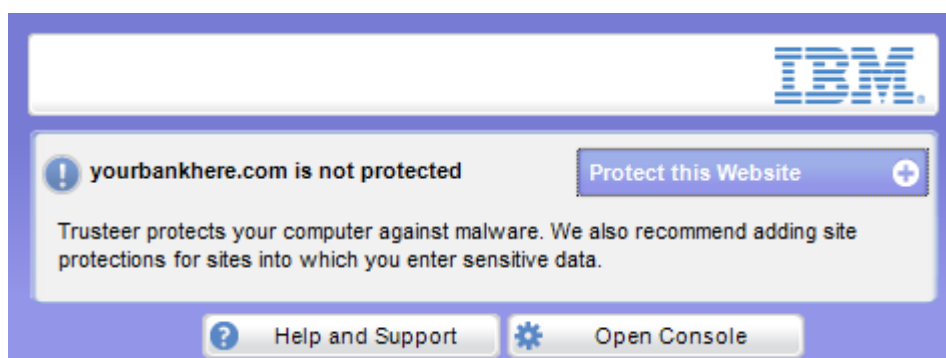
4. Pierwsze kroki

Niezwłocznie po zakończeniu instalacji program Rapport jest uruchamiany i od tego momentu wszelka komunikacja z serwisami WWW partnerów jest chroniona. Ikona programu Rapport pojawia się na pasku adresu w przeglądarce lub po jego prawej stronie. Po przejściu do serwisu WWW banku lub przedsiębiorstwa ikona programu Rapport staje się zielona, co wskazuje, że serwis jest już chroniony.



Przy pierwszym zalogowaniu się na konto bankowości elektronicznej może zostać wyświetlone okno dialogowe [ochrony hasła](#).

Po przejściu do serwisu WWW, który nie jest chroniony przez program Rapport, ikona programu Rapport jest wyszarzona. Po kliknięciu szarej ikony programu Rapport wyświetlane jest okno dialogowe (wskaźnik statusu programu Rapport) informujące, że witryna nie jest chroniona.



Dostępne możliwości to:

- [Chroń dodatkowe serwisy WWW](#), do których się logujesz, lub za pośrednictwem których możesz odczytać lub przesłać newralgiczne dane.
- [Otwórz Konsolę Rapport](#). Wiele procedur w tym podręczniku rozpoczyna się od otwarcia konsoli.
- Wybierz z nagłówek tematów te, które zawierają najbardziej interesujące informacje.

- Poczuj bezpieczeństwo podczas wykonywania czynności związanych z pracą, obsługą bankową i dokonywaniem zakupów w Internecie.

Otwórz Konsolę Rapport

Konsola Rapport to portal oferujący dostęp do szeregu funkcji i informacji dotyczących programu Rapport.

➔ Aby otworzyć Konsolę Rapport:

- Kliknij ikonę Rapport () na pasku zadań. Zostanie wyświetlona Konsola Rapport.



Nie widzę ikony programu Rapport na pasku zadań

Ikona () pojawia się domyślnie na pasku zadań programu Rapport, gdy jest on uruchomiony. Istnieje możliwość ukrycia ikony (zobacz [Ukrywanie i przywracanie ikony na pasku zadań](#)). Ikona informuje, że aktywne są zabezpieczenia programu Rapport niezależne od przeglądarki. Ochrona przeglądarki obejmuje ochronę przed szkodliwym oprogramowaniem, skanowanie i usuwanie. Jeśli ikona nie pojawia się, a nie została ona ukryta odpowiednim ustawieniem w Konsoli Rapport, oznacza to, że program Rapport nie działa. Program Rapport można zatrzymać lub zdeinstalować. Aby uruchomić program Rapport po jego zatrzymaniu, należy wybrać opcje **Programy > Trusteer Endpoint Protection > Uruchom program Trusteer Endpoint Protection**.

5. Reagowanie na alerty i ostrzeżenia

W produkcie wyświetlane są alerty i ostrzeżenia wymagające reakcji użytkownika. Po wyświetleniu okna dialogowego należy uważnie przeczytać jego treść i wybrać odpowiednią odpowiedź. Podjęcie niezbędnych działań może mieć krytyczne znaczenie dla bezpieczeństwa użytkownika. W celu odszukania danego alertu lub ostrzeżenia należy wyszukać w niniejszym dokumencie treść komunikatu wyświetlanego na ekranie.

Reagowanie na oferty ochrony hasła

Poniższy tekst stanowi przykład oferty ochrony hasła:

Program Trusteer Endpoint Protection wykrył czynność wprowadzania hasła.

Czy chcesz, aby program Trusteer Endpoint Protection rozpoczął ochronę tego hasła?

Kliknięcie opcji „Chroń to hasło” spowoduje, że program Trusteer Endpoint Protection będzie ostrzegał użytkownika przy każdej próbie wprowadzenia tego hasła w nowym serwisie WWW, w którym nie było ono dotąd wprowadzane. Pomaga to chronić przed wyłudzeniem danych logowania przez oszukańcze serwisy WWW.

Oferta ochrony hasła pojawia się jednokrotnie dla każdego chronionego serwisu WWW. Oferta ta pojawia się za pierwszym razem, gdy program Rapport wykryje czynność wprowadzania hasła w zabezpieczonym serwisie WWW. Komunikat ten zostanie wyświetlony na przykład, jeśli niedawno pobrano program Rapport z serwisu WWW banku, a następnie zalogowano się do tego serwisu WWW. Innym przykładem jest ręczne ustawienie ochrony dla serwisu WWW, a następnie zalogowanie się do niego.

W przypadku wprowadzenia objętego ochroną hasła w serwisie WWW, którego program Rapport nie rozpoznaje, [ostrzega on użytkownika](#) o próbie użycia hasła w innym serwisie WWW. Ostrzeżenie pomaga uniknąć wprowadzania hasła w oszukańczym serwisie WWW, co pomaga chronić przed [wyłudzeniem informacji](#)¹.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Chroń:** Po kliknięciu przycisku **Chroń** program Rapport rozpoczyna ochronę hasła dla tego serwisu WWW. Z chwilą zmiany hasła program Rapport, nie pytając użytkownika, automatycznie zaczyna chronić nowe hasło.
- **Nie chroń:** Wybór tej opcji powoduje, że program Rapport nie chroni żadnych haseł w tym serwisie i nie oferuje ochrony haseł w przypadku ponownych odwiedzin tego serwisu.
- **Nigdy nie chroń haseł:** Powoduje wyłączenie ochrony przed wyłudzeniem informacji przez program Rapport we wszystkich serwisach WWW. Po kliknięciu opcji **Nigdy nie chroń haseł** program Rapport nie będzie wyświetlał żadnych ostrzeżeń dotyczących wprowadzania haseł i nie będzie oferował ochrony haseł w żadnym serwisie WWW

Mam wybraną ochronę niewłaściwego hasła. Co mam teraz zrobić?

Wprowadź poprawne hasło. Program Rapport zapewni jego ochronę.

Wprowadzone przeze mnie chronione hasło zawiera błąd. Co teraz?

Ponownie poprawnie wprowadź hasło. Program Rapport umożliwi ochronę poprawnego hasła.

¹ Atak polegający na wyłudzeniu informacji to próba skłonienia użytkownika do odwiedzenia fałszywego serwisu WWW, który udaje inny, wiarygodny serwis (np. należący do banku), i wprowadzenia w nim swoich danych logowania, które mogą następnie zostać wykorzystane przez przestępców do uzyskania dostępu do konta bankowości elektronicznej i popełnienia przestępstwa, na przykład wykonania przelewu środków z rachunku bankowego użytkownika.

Mam wybraną opcję całkowitej rezygnacji z ochrony haseł, a teraz chcę chronić hasła. Co mam teraz zrobić?

Jeśli wybrano rezygnację z ochrony haseł, w strategii bezpieczeństwa programu Rapport ustawiono definicję strategii. Tę strategię można zmienić.

➔ Aby zmienić strategię ochrony haseł:

1. [Otwórz Konsole Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran User Approval. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Odszukaj element sterujący **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Z listy po prawej stronie tego elementu sterującego wybierz opcję **W newralgicznych serwisach WWW partnerów i moich** w celu zresetowania strategii i przywrócenia jej ustawień domyślnych. Zaznacz opcję **W serwisach WWW partnerów**, aby oferta ochrony haseł była wyświetlana tylko w serwisach WWW partnerów.
6. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Chcę chronić moje hasło, mimo że wcześniej została przeze mnie wybrana opcja „Nie chroń”. Jak mogę rozpocząć jego ochronę?

Możesz zmienić decyzję o ochronie hasła dla tego konkretnego serwisu.

➔ Aby włączyć wyłączoną dla konkretnego serwisu WWW ochronę hasła:

1. [Otwórz Konsolę Rapport.](#)
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Wyświetlona zostanie strategia zabezpieczeń nazw użytkowników i haseł dla każdego serwisu WWW.
6. Zaznacz pole wyboru **Ostrzegaj w przypadku użycia hasła w innym miejscu** dla serwisu WWW, dla którego ma zostać włączona ochrona hasła. Program Rapport zapewni ochronę hasła dla tego serwisu WWW.
7. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Dostaję alert o hasło, które nie jest już używane. Jak mogę to przerwać?

W zależności od naszych ustaleń z witrynami WWW partnerów, hasła są często chronione, nawet po ich zastąpieniu nowymi. Kontynuowanie ochrony haseł rzadko bywa problemem, ponieważ chronione hasła nie są używane do innych celów. Jeśli jednak wystąpi konieczność zaprzestania ochrony starego hasła przez program Rapport, można wyczyścić pamięć podręczną PII (ang. Personally Identifiable Information) w celu zresetowania mechanizmu ochrony hasła. Czyszczenie pamięci podręcznej powoduje zaprzestanie ochrony starego hasła przez program Rapport, lecz także powoduje wyświetlenie nowej oferty ochrony hasła przy następnych odwiedzinach chronionego serwisu WWW.

➔ Aby wyczyścić pamięć podręczną PII:

1. [Otwórz Konsole Rapport.](#)
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Wyświetlona zostanie strategia zabezpieczeń nazw użytkowników i haseł dla każdego serwisu WWW.
6. Kliknij opcję **Wyczyść pamięć podręczną**. Wszystkie ustawienia ochrony hasła zostaną usunięte, zaś strategie ochrony hasła zostaną zresetowane, co spowoduje ponowne wyświetlenie w programie Rapport oferty ochrony hasła przy kolejnej wizycie w każdym z serwisów WWW.

Mimo wpisania chronionego hasła w serwisie innym niż ten, dla którego mam ustawioną ochronę tego hasła, nie otrzymuję ostrzeżenia. Dlaczego?

Niektóre uprawnione serwisy zostały już przez program Rapport zidentyfikowane jako uprawnione. Ponieważ wpisanie hasła w tych serwisach nie prowadzi do oszustwa, program Rapport nie wyświetla w nich ostrzeżenia.

Reagowanie na ostrzeżenia dotyczące danych chronionych

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego danych chronionych:

Właśnie wprowadzono tekst podobny do danych logowania w serwisie: [twojbanktutaj.com](#)

Otrzymujesz to ostrzeżenie, ponieważ zamierzasz przesłać swoje dane do innego serwisu WWW: [swojbanktutaj.com](#)

Upewnij się, że rozpoznajesz serwis, do którego zamierzasz przesłać dane logowania. Dane dotyczące bezpieczeństwa mogą ulec kradzieży podczas przesyłania do nieznanego serwisu WWW.

Ostrzeżenie dotyczące ochrony danych pojawia się każdorazowo podczas wprowadzania tekstu zgodnego z chronioną nazwą użytkownika/hasłem w serwisie WWW nierozpoznawanym przez program Rapport. Celem tego okna komunikatu jest sprawdzenie, czy serwis WWW, do którego aktualnie przesyłane są informacje, nie jest serwisem oszukańczym, próbującym ukraść dane uwierzytelniające od użytkownika. Działanie takie określane jest terminem *Phishing* lub wyłudzeniem informacji.

W powyższym przykładzie program Rapport sprawdza, czy serwis WWW [swojbanktutaj.com](#) (adres przykładowy) nie podszywa się pod serwis [twojbanktutaj.com](#) i nie próbuje skłonić Cię do wprowadzenia w nim Twoich danych uwierzytelniających do serwisu [twojbanktutaj.com](#).

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zaufaj temu serwisowi:** jeśli zgadzasz się na wysłanie swoich danych logowania do tego serwisu WWW i wiesz, że ten serwis WWW nie pyta o dane uwierzytelniające innego serwisu. Po kliknięciu opcji **Zaufaj temu serwisowi** ostrzeżenie nie zostanie ponownie wyświetlone w przypadku wprowadzenia tej chronionej nazwy użytkownika lub hasła w tym serwisie WWW. Jeśli wprowadzono tekst niebędący danymi logowania lub będący danymi logowania używanymi w kilku serwisach WWW, wówczas, aby zachować możliwość wprowadzania go bez wyświetlania za każdym razem alertu, można także zaznaczyć pole wyboru **Nie chroń tych danych logowania w żadnym serwisie WWW**.

Uwaga: Sprawdzoną procedurą dotyczącą zabezpieczeń jest wybór takich haseł, które zawierają unikalne, trudne do przewidzenia frazy oraz nieużywanie tego samego hasła dla więcej niż jednego serwisu WWW. Postępowanie zgodnie z tą praktyką minimalizuje prawdopodobieństwo konieczności zaznaczenia pola wyboru **Nie chroń tych danych logowania w żadnym serwisie WWW**.

- **Zabierz mnie stąd!** Tę opcję należy wybrać, aby zrezygnować z wysyłania danych logowania do tego serwisu WWW. Zostanie wyświetlone okno dialogowe z monitem o wybranie serwisu, do którego użytkownik ma zostać przekierowany.

Dlaczego dostaję tak wiele ostrzeżeń dotyczących danych chronionych?

W przypadku użycia łańcucha znaków często wpisywanego jako hasło w wielu różnych witrynach użytkownik otrzymuje ostrzeżenie dotyczące danych chronionych każdorazowo przy wprowadzeniu tego łańcucha w dowolnym serwisie, do którego hasło jest chronione. Aby uniknąć podobnych, irytujących sytuacji, nie należy chronić haseł używanych regularnie. W przypadku używania tego rodzaju hasła w serwisie WWW, do/z którego przesyłane są newralgiczne dane, należy zmienić hasło na zapewniające wyższy poziom bezpieczeństwa. Hasło bezpieczne jest unikalne dla serwisu WWW, w którym jest używane, i składa się z sekwencji znaków trudnej do przewidzenia. Zwykle składa się ono z kombinacji liter, cyfr i symboli.

Mimo wpisania chronionego hasła w serwisie WWW nieobjętym ochroną przez program Rapport nie otrzymuję alertu. Dlaczego?

Program Rapport korzysta z szeregu metod rozpoznawania serwisów WWW jako uprawnionych. Jednak w przypadku podejrzeń, że program Rapport nie wyświetla w sposób prawidłowy alertów dotyczących konkretnego serwisu należy skontaktować się z działem wsparcia, korzystając z informacji w punkcie [Uzyskiwanie wsparcia](#).

Otrzymuję ostrzeżenie dotyczące ochrony danych mimo, że nie wpisuję chronionego hasła. Dlaczego?

W przypadku niektórych chronionych serwisów WWW program Rapport chroni wszystkie hasła wprowadzone kiedykolwiek w tym serwisie po zainstalowaniu programu Rapport. Ochrona ta obejmuje stare hasła, a nawet słowa wprowadzone przypadkowo. Może być to przyczyną wyświetlania ostrzeżenia.

Reagowanie na ostrzeżenia dotyczące wprowadzania danych bez zabezpieczenia

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego wprowadzania danych bez zabezpieczenia:

Wszelkie informacje wprowadzone na tej stronie, w tym nazwy użytkowników i hasła, są przesyłane za pośrednictwem niezaszyfrowanego połączenia i mogą zostać łatwo odczytane przez osoby trzecie.

To ostrzeżenie pojawia się przy wprowadzaniu hasła w serwisie WWW niezapewniającym bezpieczeństwa przy wprowadzaniu danych. Jest ono wyświetlane, aby ostrzec użytkownika przed przesyłaniem newralgicznych danych do serwisów o wysokim stopniu ryzyka, w tym do serwisów uprawnionych, które mogą łatwo zostać przejęte przez grupy przestępcze.

Po wyświetleniu tego komunikatu należy wybrać jedną z poniższych opcji:

- **Nie przesyłaj:** przerywa operację przesyłania i automatycznie przekierowuje przeglądarkę na stronę WWW IBM z wyjaśnieniem ryzyka związanego z wprowadzaniem danych do niezabezpieczonych serwisów.
- **Prześlij mimo to:** kontynuuje wprowadzanie mimo ostrzeżenia.
- **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie:** kontynuuje wprowadzanie mimo ostrzeżenia i zapisuje w programie Rapport informację o ufaniu temu serwisowi w przyszłości. Kliknięcie tego przycisku powoduje dodanie serwisu do listy serwisów uznawanych za zaufane. Program Rapport nie będzie ostrzegał o nich w przyszłości. Decydując się na usunięcie serwisu z listy, należy zapoznać się z informacjami w punkcie [Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych bez zabezpieczenia](#).
- **Zmień ustawienia:** otwiera ekran strategii bezpieczeństwa programu Rapport i zmienia strategię **Ostrzegaj, kiedy przesyłam newralgiczne dane do niezabezpieczonych serwisów**, decydującą o wyświetlaniu lub nie podobnych ostrzeżeń.

Czy po wybraniu opcji „Ten serwis jest zaufany, nie wyświetlaj alertu ponownie” można usunąć ten serwis z listy zaufanych serwisów?

Tak, można.

➔ Aby usunąć serwis z listy serwisów wybranych jako zaufane:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.

4. Wprowadź znaki widoczne na obrazku.
Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij element sterujący strategii **Ostrzegaj, kiedy przesyłam zabezpieczone dane do niezabezpieczonych serwisów**. Zostanie wyświetlony komunikat „Następujące serwisy wybrano jako zaufane:” wraz z listą serwisów, które wybrano jako zaufane.
6. Znajdź serwis wybrany jako zaufany i kliknij opcję **Usuń ten serwis** obok nazwy serwisu.
7. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Reagowanie na ostrzeżenia dotyczące wyłudzenia informacji

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego wyłudzenia informacji:

Próbujesz uzyskać dostęp do strony WWW pod adresem www.swojbanktutaj.com. Ten serwis WWW to znany serwis wyłudzający informacje, dlatego został on zablokowany przez program Trusteer, aby chronić dane użytkownika.

Serwisy wyłudzające informacje są tworzone przez oszustów dążących do skłonienia użytkownika do ujawnienia newralgicznych informacji przez imitowanie serwisów uprawnionych.

Wprowadzenie danych na tej stronie może skutkować kradzieżą tożsamości i stratami finansowymi.

To ostrzeżenie pojawia się po zablokowaniu przez program Rapport serwisu WWW, który użytkownik chciał odwiedzić, ponieważ program Rapport uznał ten serwis za fałszywy i znany z wyłudzenia informacji. Program Rapport wyposażono w szereg mechanizmów umożliwiających dokładne wykrycie serwisów WWW wyłudzających informacje. Ostrzeżenie to, pojawiające się po przejściu do podejrzanego serwisu

WWW, pozwala zapobiec wyłudzeniom informacji. Pojawienie się tego ostrzeżenia po kliknięciu odsyłacza do serwisu WWW oznacza, że odsyłacz jest najprawdopodobniej fałszywy, a ryzyko jest większe.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zabierz mnie stąd:** przekierowuje do poprzedniej odwiedzanej strony w przeglądarce.
- **Dlaczego ta strona była zablokowana?** Otwiera stronę WWW z wyjaśnieniem, dlaczego to ostrzeżenie zostało wyświetlone.
- **Ignoruj to ostrzeżenie:** wczytuje serwis WWW mimo zgłoszonych czynników ryzyka. Nastąpi przejście do serwisu zweryfikowanego jako serwis utworzony przez grupę przestępczą do celów oszustwa polegającego na kradzieży poufnych danych uwierzytelniających logowania do konta. W przypadku niektórych witryn wyłudzających informacje już samo wprowadzenie danych, bez naciśnięcia przycisku przesyłania, wystarcza do przechwycenia tych danych i wykorzystania ich do kradzieży lub oszustwa. Zdecydowanie zaleca się **rezygnację z wyboru tej opcji.**

Co należy zrobić, jeśli jako wyłudzający informacje został uznany serwis WWW, który uważam za uprawniony?

Jeśli serwis WWW uznany za uprawniony został oznaczony jako wyłudzający informacje, należy wykonać zrzut ekranu tego serwisu, zanotować otrzymane ostrzeżenie i otworzyć zgłoszenie na stronie <http://www.trusteer.com/support/submit-ticket>.

Jak mogę wyłączyć ostrzeżenia o zapobieganiu oszustwom?

➔ Aby wyłączyć ostrzeżenia o zapobieganiu oszustwom:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.

3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Ustaw element sterujący **Ostrzegaj przy przeglądaniu szkodliwych serwisów** na wartość **Nigdy**.
6. Kliknij przycisk **Zapisz**. Zmiana dotycząca strategii zabezpieczeń zostanie zapisana.

Reagowanie na ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej

Poniższy tekst stanowi przykład ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej:

Prawdopodobnie wprowadzasz dane karty płatniczej w serwisie WWW niezabezpieczonym lub o wysokim stopniu ryzyka. Nie zaleca się wprowadzania danych kart płatniczych w niezabezpieczonych serwisach.

To ostrzeżenie pojawia się podczas wprowadzania zabezpieczonych numerów kart płatniczych na stronie WWW na dysku lokalnym lub w dowolnym niezabezpieczonym serwisie WWW. Ten komunikat jest wyświetlany z myślą o tym, aby pomóc użytkownikowi uniknąć przesyłania numerów kart płatniczych do oszukańczych serwisów lub do serwisów uprawnionych, lecz nie zapewniających odpowiedniego poziomu bezpieczeństwa.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zabierz mnie z tej strony:** tę opcję należy wybrać w przypadku rezygnacji z wysyłania danych karty do tego serwisu WWW. W przeglądarce zostanie załadowana strona startowa.
- **Ignoruj, ten serwis WWW jest zaufany:** tę opcję należy wybrać, aby przesłać dane karty do tego serwisu WWW. Okno dialogowe zostanie zamknięte, lecz program Rapport będzie nadal blokował możliwość przechwycenia danych karty płatniczej przez programy rejestrujące naciśnięcia klawiszy. Wystawca karty płatniczej otrzymuje powiadomienie o tym wyborze. Decydując się na usunięcie strony wybranej wcześniej jako zaufana, należy zapoznać się z informacjami w punkcie [Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych kart płatniczych](#).

Uwaga: Zignorowanie tego ostrzeżenia spowoduje wysłanie danych karty płatniczej do znanego oszukańczego serwisu WWW lub wysłanie ich do serwisu, który nie zapewnia szyfrowania i pozwala na ich ujawnienie podmiotom trzecim.

- **Zawsze ufaj tej witrynie:** program Rapport ufa obecnie tej witrynie i nie wyświetla tego ostrzeżenia ponownie przy próbie wprowadzenia przez użytkownika w tym serwisie jakiegokolwiek numeru karty płatniczej. Program Rapport będzie nadal blokował możliwość przechwycenia danych karty płatniczej przez programy rejestrujące naciśnięcia klawiszy.
- **Zrezygnuj z ochrony kart:** wyłącza funkcję ochrony kart płatniczych. Aby ponownie włączyć tę funkcję, zmień wartość ustawienia dla strategii **Chroń numery kart płatniczych przed kradzieżą z Nigdy na Zawsze**.

Uwaga: Ochrona kart płatniczych jest włączona tylko dla systemów kart płatniczych objętych taką ochroną.

Reagowanie na komunikaty o ochronie karty płatniczej

Poniższy tekst stanowi przykład komunikatu o ochronie karty płatniczej:

Prawdopodobnie wprowadzasz dane karty płatniczej. Firma Trusteer automatycznie zabezpiecza dane karty płatniczej przed kradzieżą online.

Ten komunikat informuje użytkownika o tym, że program Rapport wykrył operację przesyłania numeru karty płatniczego do strony WWW i rozpoczął szyfrowanie danych wprowadzanych na stronie, aby uniemożliwić przechwycenie numeru karty płatniczej przez szkodliwe oprogramowanie rejestrujące naciśnięcia klawiszy. Komunikat ten jest wyświetlany po wprowadzeniu numeru chronionej karty płatniczej w chronionym serwisie WWW programu Rapport lub w dowolnym chronionym (za pomocą protokołu https) serwisie zawierającym słowo kluczowe związane z kartą płatniczą, takim jak Visa, Mastercard czy Amex.

Po wyświetleniu tego komunikatu nie trzeba już robić nic więcej. Opcjonalnie można kliknąć przycisk **OK** w celu zamknięcia okna z komunikatem. W przypadku rezygnacji okno zostanie zamknięte automatycznie po krótkim czasie.

Jeśli nie chcesz otrzymywać powiadomień o aktywacji funkcji blokującej rejestrację naciśnięć klawiszy, kliknij opcję **Nie wyświetlaj tego komunikatu ponownie**. Aby ponownie włączyć te powiadomienia, zaznacz dla strategii **Chroń numery kart płatniczych przed kradzieżą** pole wyboru **Powiadom mnie o aktywacji zabezpieczeń kart płatniczych przez program Trusteer**.

Uwaga: Ochrona kart płatniczych jest włączona tylko dla [systemów kart płatniczych objętych taką ochroną](#).

Reagowanie na alerty o wykryciu próby wykonania zrzutu ekranu

Poniższy tekst stanowi przykład alertu dotyczącego wykrycia próby wykonania zrzutu ekranu:

*Przechwycony ekran może zawierać newralgiczne dane z serwisu
twojbanktutaj.com*

Ten alert pojawia się, gdy na komputerze w chwili wyświetlania serwisu WWW partnera zostanie naciśnięty klawisz PrtScn. Alert pomaga zdecydować o zablokowaniu lub zezwoleniu na wykonanie zrzutu ekranu.

Klawisz PrtScn na klawiaturze służy do wykonywania zrzutów ekranu. Możliwe jest jednak aktywowanie przez szkodliwe oprogramowanie tego samego mechanizmu, aktywowanego przez ten klawisz, i przechwycenie newralgicznych informacji w celu dokonania oszustwa.

Uwaga: Ten alert jest generowany przez funkcję blokowania przechwytywania ekranu, włączaną domyślnie w serwisach WWW partnerów.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Zezwalaj:** umożliwia przechwycenie ekranu za pomocą klawisza PrtScn. Tę opcję należy wybrać w przypadku celowego naciśnięcia klawisza zrzutu ekranu w celu jego przechwycenia.
- **Blokuj:** uniemożliwia przechwycenie ekranu za pomocą klawisza PrtScn. Wybierz tę opcję, jeśli klawisz PrtScn został naciśnięty nieumyślnie.

To okno dialogowe jest wyświetlane nawet wówczas, jeśli nie próbuję wykonać zrzutu ekranu zawierającego newralgiczne dane.

Zminimalizuj lub zamknij wszystkie okna przeglądarki i spróbuj ponownie.

Reagowanie na alerty dotyczące ochrony przeglądarki

Poniższy tekst stanowi przykład alertu dotyczącego ochrony przeglądarki:

Poniższy dodatek programu Internet Explorer korzysta z nieznanej metody dostępu do przeglądarki i jako taki nie podlega monitorowaniu przez program Trusteer Endpoint Protection. Ten pasek narzędzi można albo na stałe włączyć, albo zablokować.

Ten alert pojawia się, gdy program dodatkowy (taki jak pasek narzędzi lub rozszerzenie) próbuje uzyskać dostęp do informacji należących do chronionego serwisu WWW za pomocą metody, która nie jest obecnie monitorowana w programie Rapport.

Po wyświetleniu tego alertu należy wybrać jedną z poniższych opcji:

- **Zezwól na stałe:** powoduje zezwolenie na działanie programu dodatkowego w dowolnym serwisie WWW. Wybierz tę opcję, jeśli wiesz o działaniu programu dodatkowego w swojej przeglądarce, korzystasz z niego i ufasz jego źródłu.
- **Blokuj na stałe:** powoduje zablokowanie przez program Rapport działania programu dodatkowego w dowolnym serwisie WWW i powoduje anonimowe przesłanie do IBM raportu dotyczącego bezpieczeństwa o zablokowanym programie dodatkowym, umożliwiając przeanalizowanie tego faktu przez ekspertów ds. bezpieczeństwa IBM. Pozwala to IBM globalnie i na stałe zablokować program dodatkowy, jeśli zostanie on zidentyfikowany jako szkodliwy.

Czy mogę odblokować zablokowany wcześniej przez siebie program dodatkowy lub zablokować program dodatkowy, na którego działanie została wcześniej wyrażona zgoda?

➔ Aby zmienić status programów dodatkowych, na których działanie zezwolono lub które zablokowano:

1. [Otwórz Konsole Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.

3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij nazwę strategii **Blokuj nieznane programy dodatkowe w przeglądarce**. Poniżej nazwy strategii zostanie wyświetlona lista wszelkich dozwolonych lub zablokowanych programów dodatkowych.
6. Przełącz status zablokowania lub zezwolenia każdego z programów dodatkowych stosownie do potrzeb.
7. Kliknij przycisk **Zapisz**. Zmiany zostaną zapisane.

Reagowanie na alerty dotyczące aktywacji funkcji usuwania szkodliwego oprogramowania

Poniższy tekst stanowi przykład alertu dotyczącego aktywacji funkcji usuwania szkodliwego oprogramowania:

Program Trusteer Endpoint Protection wykrył i zablokował szkodliwe oprogramowanie <nazwa_szkodliwego_oprogramowania>. Usunięcie szkodliwego oprogramowania przerwano, ponieważ dla strategii usuwania szkodliwego oprogramowania wybrano wartość „Nigdy”.

NALEŻY TERAZ AKTYWOWAĆ STRATEGIĘ USUWANIA SZKODLIWEGO OPROGRAMOWANIA W CELU ZMAKSYMALIZOWANIA POZIOMU BEZPIECZEŃSTWA.

Ten alert pojawia się po wyłączeniu strategii usuwania szkodliwego oprogramowania, po wykryciu i zablokowaniu go przez program Rapport. Alert ten ma stanowić zachętę do aktywacji przez użytkownika strategii usuwania szkodliwego oprogramowania, tak aby program Rapport mógł usunąć szkodliwe oprogramowanie. Usuwanie szkodliwego oprogramowania włączono domyślnie, lecz można je wyłączyć, korzystając ze strategii bezpieczeństwa programu Rapport.

Po wyświetleniu tego alertu należy wybrać jedną z poniższych opcji:

- **Aktywuj strategię usuwania teraz:** strategia usuwania szkodliwego oprogramowania zostaje aktywowana i program Rapport inicjuje usuwanie zablokowanego szkodliwego oprogramowania. Może zostać wyświetlone inne okno dialogowe wymagające zrestartowania komputera. Użytkownik przed kliknięciem przycisku **Zrestartuj komputer teraz** będzie miał możliwość zapisania i zamknięcia otwartych plików i aplikacji. Proces restartowania kończy usuwanie szkodliwego oprogramowania.
- **Ignoruj:** Alert ten pojawia się przy następnej próbie wykrycia szkodliwego oprogramowania przez program Rapport. Szkodliwe oprogramowanie pozostaje na komputerze, lecz jest zablokowane. Zablokowane szkodliwe oprogramowanie znajdujące się na komputerze stanowi ryzyko, ponieważ może ono zostać aktywowane w przyszłości, w sytuacji zatrzymania lub zdeinstalowania programu Rapport albo w sytuacji użycia przeglądarki nieobsługującej programu Rapport.

Reagowanie na alerty dotyczące zainicjowania usuwania szkodliwego oprogramowania

Poniższy tekst stanowi przykład alertu dotyczącego zainicjowania usuwania szkodliwego oprogramowania:

*Program Trusteer Endpoint Protection wykrył i zablokował szkodliwe oprogramowanie <nazwa_szkodliwego_oprogramowania>; zainicjowano usuwanie szkodliwego oprogramowania.
ZRESTARTUJ TERAZ KOMPUTER, ABY UKOŃCZYĆ USUWANIE*

Alert podobny do powyższego pojawia się po wykryciu i zablokowaniu przez program Rapport szkodliwego oprogramowania i przystąpieniu do usuwania go z komputera. Do ukończenia procesu usuwania szkodliwego oprogramowania przez program Rapport konieczne jest zrestartowanie komputera.

Po wyświetleniu tego alertu należy wybrać jedną z poniższych opcji:

- **Zrestartuj komputer teraz:** restartuje komputer niezwłocznie, po ukończeniu procesu usuwania szkodliwego oprogramowania. Po zrestartowaniu komputera i zalogowaniu się na swoje konto w serwisie chronionym przez program Rapport upewnij się, że ikona programu Rapport jest zielona. Alert dotyczący zainicjowania usuwania szkodliwego oprogramowania nie powinien pojawić się ponownie po zrestartowaniu komputera. Jeśli pojawi się on ponownie, należy przesłać raport dotyczący problemu z Konsoli Rapport.
- **Ignoruj:** Usuwanie szkodliwego oprogramowania zostanie zakończone przy kolejnej próbie zrestartowania komputera. Do chwili zrestartowania komputera należy unikać wszelkich newralgicznych operacji online. Program Rapport nie wyświetli ponownego alertu dotyczącego usuwania tego szkodliwego oprogramowania.

- **Zawieś wyświetlanie alertu na tydzień:** ten alert zostanie wyświetlony ponownie w ciągu tygodnia, jeśli szkodliwe oprogramowanie nie zostanie wcześniej usunięte. Jeśli w tym czasie komputer zostanie zrestartowany, proces usuwania szkodliwego oprogramowania zostanie zakończony i alert nie pojawi się ponownie.

Reagowanie na ostrzeżenia dotyczące niepoprawnego certyfikatu

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego niepoprawnego certyfikatu:

*Ten serwis WWW korzysta z niepoprawnego certyfikatu.
Zaleca się zablokowanie dostępu do tego serwisu WWW, o ile nie jest on
wewnętrznym serwisem organizacji użytkownika.*

To ostrzeżenie pojawia się po przejściu do chronionego serwisu WWW, po wykryciu przez program Rapport, że [certyfikat²](#) serwisu WWW jest niepoprawny. Nieważny certyfikat mógł utracić ważność, może być niepoprawny lub podpisany przez nieznanego wystawcę. To ostrzeżenie jest wyświetlane, aby ostrzec użytkownika przed wysyłaniem newralgicznych danych do oszukańczych serwisów WWW.

Uwaga: To ostrzeżenie może pojawiać się na stronach WWW z poprawnymi certyfikatami, jeśli datę lub godzinę dla tego komputera ustawiono nieprawidłowo. W przypadku częstego pojawiania się tego ostrzeżenia należy sprawdzić datę i godzinę na komputerze.

Ostrzeżenie dotyczące nieważnego certyfikatu zawiera następujące informacje:

² Certyfikat SSL to kryptograficzny certyfikat cyfrowy potwierdzający tożsamość serwisu WWW i tworzący zaszyfrowane połączenie umożliwiające przesyłanie newralgicznych danych do serwisu WWW. Symbol kłódki na pasku adresu przeglądarki lub w dolnej części przeglądarki oznacza, że połączenie między przeglądarką a serwisem WWW jest zabezpieczone protokołem SSL. Jednocześnie jednak obecność symbolu kłódki nie gwarantuje, że certyfikat jest poprawny.

Pole na ekranie	Opis
Przyczyna błędu	Przyczyna aktywacji tego ostrzeżenia przez program Rapport. Możliwe wartości: • Adresy są niezgodne: adres, do którego próbowano uzyskać dostęp, i adres na certyfikacie są niezgodne. Aby certyfikat był ważny, adresy muszą być zgodne. Sprawdź oba adresy. Jeśli adres na certyfikacie wydaje się podejrzany lub niepowiązany z serwisem WWW, do którego usiłujesz uzyskać dostęp, zdecyduj o zablokowaniu dostępu. • Nieznany podmiot podpisujący certyfikat: podmiot, który podpisał certyfikat, jest nieznany IBM. Nie należy ufać nieznanym podmiotom podpisującym przy generowaniu ważnych certyfikatów. Banki i instytucje finansowe zawsze korzystają z certyfikatów od znanych osób podpisujących. • Certyfikat utracił ważność: certyfikat utracił ważność i nie jest poprawny. Serwis WWW korzystający z certyfikatu, który utracił ważność, cechuje niski poziom bezpieczeństwa. Banki i instytucje finansowe nigdy nie korzystają z certyfikatów, które utraciły ważność. Sprawdź zegar systemowy, aby upewnić się, że data na komputerze jest poprawna. Jeśli na komputerze ustawiona jest data z przyszłości, ten komunikat może być wyświetlany w wyniku błędu. • Niepoprawny certyfikat: Format certyfikatu jest niepoprawny.
Adres na certyfikacie	Adres na certyfikacie wyświetlanym przez ten serwis WWW. Każdy certyfikat jest wydawany dla konkretnego adresu WWW. W serwisie WWW powinien być widoczny certyfikat z listą posiadanych adresów.
Adres we wniosku	Adres WWW, pod który przekierowywana jest przeglądarka. Jest to adres, do którego próbowano uzyskać dostęp.
Data ważności certyfikatu	Każdy certyfikat jest ograniczony w czasie. Serwis WWW korzystający z certyfikatu, który utracił ważność, cechuje niski poziom bezpieczeństwa.
Osoba podpisująca	Podmiot, który wystawił certyfikat. Nie należy ufać certyfikatom od nieznanym podmiotów.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Blokuj dostęp.** Blokuje dostęp do serwisu. Wybierz tę opcję, jeśli serwis WWW jest serwisem o charakterze finansowym lub zakupowym, do którego użytkownicy przesyłają newralgiczne informacje.
- **Zezwalaj na dostęp.** Umożliwia dostęp do serwisu. Tę opcję można wybrać, jeśli serwis WWW znajduje się w sieci lokalnej (intranet) lub jeśli nie operuje on newralgicznymi informacjami. W przypadku zezwolenia na dostęp należy postępować z zachowaniem ostrożności i nie przysyłać do serwisu newralgicznych informacji. Pole wyboru **Nie wyświetlaj ostrzeżenia dotyczącego tego serwisu WWW ponownie** należy zaznaczyć tylko, jeśli program Rapport nie powinien wyświetlać alertów dotyczących tego serwisu w przyszłości.

Jak mogę wyłączyć tę funkcję?

Istnieje możliwość wyłączenia sprawdzania poprawności certyfikatu SSL za pomocą Konsoli Rapport. Powoduje to zatrzymanie mechanizmu sprawdzania przez program Rapport ważności certyfikatów serwisów WWW, a w efekcie przerwanie pojawiania się tych ostrzeżeń.

➔ Aby wyłączyć sprawdzanie poprawności certyfikatu SSL:

1. [Otwórz Konsolę Rapport.](#)
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Odszukaj element sterujący **Sprawdź poprawność certyfikatów SSL serwisu WWW**.
6. Z listy po prawej stronie tego elementu sterującego wybierz opcję **Nigdy**.
7. Kliknij przycisk **Zapisz**. Sprawdzanie poprawności certyfikatu SSL jest teraz wyłączone.

Reagowanie na standardowe ostrzeżenia dotyczące konta użytkownika

Poniższy tekst stanowi przykład standardowego ostrzeżenia dotyczącego konta użytkownika:

Program Trusteer Endpoint Protection zidentyfikował na tym komputerze szkodliwe oprogramowanie stwarzające wysokie ryzyko dla operacji finansowych. Zaleca się powstrzymanie od wykonywania operacji bankowych na tym konkretnym komputerze aż do chwili rozwiązania problemu lub aż do chwili ponownego zainstalowania programu Trusteer Endpoint Protection za pośrednictwem konta użytkownika systemu Windows z uprawnieniami administratora.

To ostrzeżenie pojawia się podczas instalowania programu Rapport za pośrednictwem standardowego konta użytkownika, znanego także jako konto użytkownika z ograniczeniami (ang. Limited User Account, LUA). W przypadku zainstalowania programu Rapport za pośrednictwem standardowego konta użytkownika nie jest możliwe uruchomienie zaawansowanych funkcji usuwania szkodliwego oprogramowania i komputer może być wystawiony na ryzyko. Do zapewnienia pełnej ochrony komputera program Rapport wymaga uprawnień administratora.

Należy spróbować zainstalować program Rapport ponownie, korzystając z uprawnień administratora. W przypadku braku uprawnień administratora należy skontaktować się z administratorem IT.

Więcej informacji można znaleźć na stronie:

<http://manage.trusteer.com/support/what-admin-mode-windows>

Reagowanie na powiadomienia dotyczące raportu o aktywności

Poniższy tekst stanowi przykład powiadomienia dotyczącego tygodniowego raportu o aktywności:

Okresowy raport o aktywności jest gotowy.

To powiadomienie pojawia się raz na tydzień w przypadku wybrania w Konsoli Rapport opcji [generowania tygodniowego raportu o aktywności](#).

Po wyświetleniu tego powiadomienia należy wybrać jedną z poniższych opcji:

- **Otwórz raport:** otwiera Konsolę Rapport i wyświetla tygodniowy raport o aktywności.
- **Zamknij:** zamyka alert i nie wyświetla raportu o aktywności. [Raport o aktywności](#) można jednak wyświetlić w dowolnej chwili.

Minął ponad tydzień, a nadal nie otrzymuję powiadomienia o dostępności Tygodniowego raportu o aktywności. Dlaczego?

Tygodniowy raport o aktywności pojawia się tylko, jeśli w ciągu ostatniego tygodnia miało miejsce co najmniej jedno zdarzenie. Istnieje możliwość, że nie zarejestrowano żadnych zdarzeń.

Reagowanie na komunikaty o potwierdzeniu aktualizacji kodu

W przypadku włączenia na komputerze kontroli konta użytkownika (funkcja zabezpieczeń dostępna w systemach Windows 8 i Windows 7) od czasu do czasu podczas automatycznej aktualizacji programu Rapport może być widoczny następujący komunikat:

Ukończenie procesu aktualizacji oprogramowania wymaga zastąpienia przez program Trusteer Endpoint Protection plików aplikacji. W systemie operacyjnym może zostać wyświetlone okno dialogowe z potwierdzeniem. Kliknij przycisk potwierdzania, aby pomyślnie ukończyć proces aktualizacji.

W przypadku wyświetlenia tego komunikatu kliknij przycisk **OK**. Następnie może zostać wyświetlone okno dialogowe Kontrola konta użytkownika z informacją o konieczności dysponowania uprawnieniami do kontynuowania procesu aktualizacji programu Rapport. Po wyświetleniu komunikatu Kontrola konta użytkownika należy kliknąć przycisk **Kontynuuj** w celu ukończenia procesu aktualizacji.

Uwaga: Jeśli komunikat z potwierdzeniem aktualizacji kodu pojawia się często, należy przesłać wniosek o wsparcie na stronie:
<http://www.trusteer.com/support/submit-ticket>.

Reagowanie na ostrzeżenia dotyczące trybu zgodności z lektorem ekranowym

Poniższy tekst stanowi przykład ostrzeżenia dotyczącego trybu zgodności z lektorem ekranowym:

Program Trusteer Endpoint Protection jest obecnie zainstalowany w trybie zgodności z lektorem ekranowym. Aktywowanie tej strategii może spowodować wyłączenie niektórych lektorów ekranowych. Czy na pewno chcesz aktywować tę strategię?

To ostrzeżenie pojawia się, jeśli program Rapport jest zainstalowany w trybie zgodności z lektorem ekranowym, podczas próby włączenia jednej z następujących strategii bezpieczeństwa:

- **Blokuj wykonywanie zrzutów ekranu**
- **Blokuj dostęp do informacji w przeglądarce**

Te strategie są domyślnie wyłączone, jeśli program został zainstalowany w trybie zgodności z lektorem ekranowym. Włączenie którejkolwiek z tych strategii może spowodować zakłócenia w działaniu oprogramowania lektora ekranowego, uniemożliwiając mu odczytywanie stron WWW oraz opcji menu i okien dialogowych programu Rapport.

Po wyświetleniu tego ostrzeżenia należy wybrać jedną z poniższych opcji:

- **Aktywuj strategię.** Tę opcję należy wybrać w przypadku pewności co do zamiaru włączenia strategii, jeśli nie ma ryzyka, że uniemożliwi to korzystanie z lektorów ekranowych w programie Rapport.

Uwaga: Jeśli nie ma potrzeby korzystania z lektorów ekranowych, należy zainstalować program Rapport ponownie, nie wybierając trybu zgodności z lektorem ekranowym. Przed ponowną instalacją należy usunąć wszystkie foldery powiązane z programem Rapport. Wskazówki dotyczące usuwania folderów można znaleźć tutaj:
<http://www.trusteer.com/support/remove-rapport-folders>

- **Anuluj.** Tę opcję należy wybrać, aby anulować operację aktywacji strategii.

Reagowanie na alerty dotyczące ponownej instalacji w trybie administratora

Poniższy tekst stanowi przykład alertu dotyczącego ponownej instalacji w trybie administratora:

Program Trusteer Endpoint Protection zainstalowano uprzednio za pośrednictwem konta o ograniczonych uprawnieniach użytkownika. W celu zmaksymalizowania bezpieczeństwa zaleca się ponowne zainstalowanie programu Trusteer Endpoint Protection z konta użytkownika dysponującego uprawnieniami administratora.

Ten alert wskazuje, że usługodawca udostępniający program Rapport ograniczył w ostatnim czasie możliwość instalowania programu Rapport do kont z uprawnieniami administratora systemu Windows. Program Rapport został zainstalowany za pośrednictwem standardowego konta użytkownika. Dostawca zaleca obecnie zdeinstalowanie programu Rapport za pośrednictwem standardowego konta użytkownika, na którym zainstalowano program Rapport, a następnie ponowną instalację programu Rapport za pośrednictwem konta administratora. Po zainstalowaniu programu Rapport za pośrednictwem konta administratora stanie się on aktywny na wszystkich kontach użytkowników systemu Windows na komputerze.

Konto administratora systemu Windows jest kontem użytkownika systemu Windows, które umożliwia dokonywanie zmian mających wpływ na ustawienia wszystkich lub wybranych użytkowników danego komputera. Zmiany te uwzględniają ustawienia zabezpieczeń, procesy instalacji oprogramowania i dostęp do plików. Mimo że każdy komputer z systemem Windows ma konto administratora, Microsoft zaleca korzystanie ze standardowego konta użytkownika przy zwykle wykonywanych operacjach.

Po wyświetleniu tego alertu należy wybrać jedną z następujących opcji:

- **Zamknij.** Następuje zamknięcie alertu. Następnie można ponownie zainstalować program Rapport, korzystając z poniższej procedury.
- **Wyświetl alert po 7 dniach.** Alert zostaje zamknięty, a następnie jest wyświetlany ponownie po upływie siedmiu dni w celu przypomnienia użytkownikowi o konieczności przeprowadzenia ponownej instalacji.

➔ **Aby ponownie zainstalować program Rapport:**

1. Zdeinstaluj program Rapport, korzystając z tego samego standardowego konta użytkownika, które było używane do zainstalowania programu Rapport:

- [Deinstalowanie programu Rapport \(Windows 8 i Windows 7\)](#)
- [Deinstalowanie programu Rapport \(Windows XP\)](#)

Uwaga: W oknie dialogowym Deinstalowanie programu IBM Security Trusteer Endpoint Protection należy zaznaczyć pole wyboru **Usuń ustawienia wszystkich użytkowników**. Jest to niezbędne do zapewnienia bezproblemowej ponownej instalacji.

2. Przełącz się na konto administratora:

- [Przełączanie się na konto administratora \(system operacyjny Windows 8\)](#)
- [Przełączanie się na konto administratora \(system operacyjny Windows 7\)](#)
- [Przełączanie się na konto administratora \(system operacyjny Windows XP\)](#)

3. Należy pobrać najnowszą wersję programu Rapport od swojego usługodawcy; w tym celu:
 - a. Przejdź na stronę <http://www.trusteer.com/support/rapport-installation-links>.
 - b. Odszukaj odpowiedni dla swojego usługodawcy (banku, przedsiębiorstwa lub innej organizacji, która zaoferowała Ci program Rapport) odsyłacz do pliku do pobrania.
 - c. Kliknij odsyłacz do pliku instalacyjnego do pobrania.
 - d. Po wyświetleniu monitu zapisz plik na komputerze.
 - e. Uruchom plik, aby go zainstalować. Pełną instrukcję instalacji można znaleźć w sekcji [Instalowanie programu Rapport](#).

Przełączanie się na konto administratora (system operacyjny Windows 8)

Aby przełączyć się na konto administratora, potrzebne są nazwa użytkownika i hasło dla konta administratora. Jeśli nie znasz nazwy użytkownika ani hasła dla konta administratora, musisz zwrócić się do administratora z prośbą o zmianę rodzaju swojego konta lub zainstalowanie programu Rapport.

➔ Aby przełączyć się na konto użytkownika o uprawnieniach administratora:

1. Na ekranie **Start** kliknij ikonę konta.
2. Klikając, wybierz użytkownika, na którego konto chcesz się przełączyć.

Nie wiem, czy konto, którego używam, jest kontem administratora

Jeśli nie masz pewności, czy konto użytkownika jest kontem administratora, czy standardowym kontem użytkownika, możesz sprawdzić typ konta, przełączając się na nie, a następnie wykonując poniższe czynności.

➔ Jeśli komputer należy do domeny:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.

3. Kliknij opcję **Konta użytkowników**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj kontami użytkowników**.
6. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Nazwa użytkownika jest podświetlona, zaś typ konta jest wyświetlony w kolumnie Grupa.

➔ **Jeśli komputer należy do grupy roboczej:**

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników i bezpieczeństwo rodzinne**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj innym kontem**. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika.) Typ konta jest wyświetlany pod nazwą użytkownika.

Przełączanie się na konto administratora (system operacyjny Windows 7)

Aby przełączyć się na konto administratora, potrzebne są nazwa użytkownika i hasło dla konta administratora. Jeśli nie znasz nazwy użytkownika ani hasła dla konta administratora, musisz zwrócić się do administratora z prośbą o zmianę rodzaju swojego konta lub zainstalowanie programu Rapport.

➔ **Aby przełączyć się na konto użytkownika o uprawnieniach administratora:**

1. Kliknij **Start**.
2. Kliknij strzałkę obok opcji **Zamknij**.

3. Kliknij opcję **Przełącz użytkownika**.
4. Naciśnij kombinację klawiszy **Ctrl+Alt+Delete**, a następnie kliknij konto użytkownika, na które chcesz się przełączyć.

Nie wiem, czy konto, którego używam, jest kontem administratora

Jeśli nie masz pewności, czy konto użytkownika jest kontem administratora, czy standardowym kontem użytkownika, możesz sprawdzić typ konta, przełączając się na nie, a następnie wykonując poniższe czynności.

➔ Jeśli komputer należy do domeny:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj kontami użytkowników**.
6. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Nazwa użytkownika jest podświetlona, zaś typ konta jest wyświetlony w kolumnie Grupa.

➔ Jeśli komputer należy do grupy roboczej:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników i bezpieczeństwo rodzinne**.
4. Kliknij opcję **Konta użytkowników**.

5. Kliknij opcję **Zarządzaj innym kontem**. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Typ konta jest wyświetlany pod nazwą użytkownika.

Przełączanie się na konto administratora (system operacyjny Windows XP)

Aby przełączyć się na konto administratora, potrzebne są nazwa użytkownika i hasło dla konta administratora. Jeśli nie znasz nazwy użytkownika ani hasła dla konta administratora, musisz zwrócić się do administratora z prośbą o zmianę rodzaju swojego konta lub zainstalowanie programu Rapport.

➔ Aby przełączyć się na konto użytkownika o uprawnieniach administratora:

- Jeśli włączono opcję Szybkie przełączanie (opcja domyślna w przypadku systemów operacyjnych Windows XP Home Edition i Professional na komputerach wyposażonych w ponad 64 MB pamięci RAM):
 1. Kliknij **Start**.
 2. Kliknij opcję **Wyloguj**.
 3. Kliknij opcję **Przełącz użytkownika**. Zostanie wyświetlony ekran logowania systemu operacyjnego Windows XP wraz z liczbą programów dla każdego użytkownika pod nazwą użytkownika.
 4. Klikając, wybierz użytkownika, na którego konto chcesz się przełączyć.
 5. Wpisz hasło, a następnie kliknij strzałkę, aby zalogować się na komputerze.
- Jeśli opcja Szybkie przełączanie jest wyłączona lub nie jest obsługiwana (w przypadku komputerów z systemem operacyjnym Windows XP Professional będących częścią domeny):
 1. Zrestartuj komputer
 2. Zaloguj się, korzystając z nazwy użytkownika i hasła użytkownika o uprawnieniach administratora.

Nie wiem, czy konto, którego używam, jest kontem administratora

Jeśli nie masz pewności, czy konto użytkownika jest kontem administratora, czy standardowym kontem użytkownika, możesz sprawdzić typ konta, przełączając się na nie, a następnie wykonując poniższe czynności.

➔ Jeśli komputer należy do domeny:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj kontami użytkowników**.
6. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Nazwa użytkownika jest podświetlona, zaś typ konta jest wyświetlony w kolumnie Grupa.

➔ Jeśli komputer należy do grupy roboczej:

1. Kliknij **Start**.
2. Kliknij opcję **Panel sterowania**.
3. Kliknij opcję **Konta użytkowników i bezpieczeństwo rodzinne**.
4. Kliknij opcję **Konta użytkowników**.
5. Kliknij opcję **Zarządzaj innym kontem**. Po wyświetleniu zachęty do wprowadzenia hasła administratora lub potwierdzenia wpisz hasło lub potwierdź. (Jeśli hasło nie zostanie zaakceptowane, możesz założyć, że używane konto jest standardowym kontem użytkownika). Typ konta jest wyświetlany pod nazwą użytkownika.

6. Dostosowywanie programu Rapport

Można zmienić język Konsoli Rapport oraz okien dialogowych oraz ukryć ikonę programu Rapport pojawiającą się obok paska adresu przeglądarki, a także ukryć ikonę programu Rapport wyświetlaną na pasku zadań.

Ukrywanie i przywracanie ikony programu Rapport na pasku adresu

Domyślnie ikona programu Rapport zawsze pojawia się na pasku adresu przeglądarki lub po jego prawej stronie. Ikona ma kolor zielony, jeśli serwis WWW w przeglądarce jest chroniony przez program Rapport, a kolor szary, jeśli serwis WWW w przeglądarce nie jest chroniony przez program Rapport.



Poza wskazaniem chronionych serwisów WWW można kliknąć ikonę programu Rapport i wybrać opcję **Chroń ten serwis WWW**, aby włączyć ochronę niechronionego serwisu.

Ikony tę można ukryć, jeśli jest to preferowane. Gdy ikona programu Rapport jest ukryta, program Rapport kontynuuje udostępnianie tego samego zabezpieczenia dla chronionych serwisów WWW, lecz nie jest widoczne, które serwisy WWW są chronione, i nie można zdecydować o włączeniu ochrony dla niechronionego serwisu WWW.

Wyświetlaniem lub ukrywaniem ikony można sterować z poziomu Konsoli Rapport. Jeśli ikona jest ukryta, dostęp do Konsoli Rapport można uzyskać wyłącznie z menu Start systemu Windows.

➔ Aby ukryć ikonę programu Rapport:

1. [Otwórz Konsolę Rapport](#).
2. W obszarze Ustawienia produktu panelu kontrolnego, obok statusu **Ikona na pasku adresu** kliknij opcję **ukryj**. Zostanie wyświetlone okno komunikatu następującej treści:

Aby zmiany odniosły skutek, może być konieczne zamknięcie i ponowne otwarcie przeglądarki.

3. Kliknij przycisk **OK**. Status **Ikona na pasku adresu** zmieni się na ukryty i zostanie wyświetlony odsyłacz **pokaż**.

Ikona jest teraz ukryta lub zostanie ukryta po zrestartowaniu przeglądarki.

➔ Aby przywrócić ikonę:

- Kliknij przycisk **pokaż**.

Ukrywanie i przywracanie ikony na pasku zadań

Domyślnie ikona programu Rapport () pojawia się na pasku zadań zawsze, gdy program Rapport jest uruchomiony.

Ikona informuje, że aktywne są zabezpieczenia programu Rapport niezależne od przeglądarki. Ochrona ta obejmuje ochronę przed szkodliwym oprogramowaniem, skanowanie i usuwanie go. Aby otworzyć Konsolę Rapport, należy kliknąć ikonę Rapport.

Ikona tę można ukryć, jeśli jest to preferowane. Mimo że ikona programu Rapport jest ukryta, program Rapport zapewnia ten sam poziom ochrony.

Wyświetlaniem lub ukrywaniem ikony można sterować z poziomu Konsoli Rapport. Jeśli ikona jest ukryta, dostęp do Konsoli Rapport można uzyskać wyłącznie z menu Start systemu Windows.

➔ Aby ukryć ikonę programu Rapport wyświetlaną na pasku zadań:

1. [Otwórz Konsolę Rapport.](#)
2. W obszarze Ustawienia produktu panelu kontrolnego obok statusu **Ikona na pasku zadań** kliknij opcję **ukryj**. Status **Ikona na pasku zadań** zmieni się na ukryty i zostanie wyświetlony odsyłacz **pokaż**.

Ikona jest teraz ukryta na pasku zadań.

➔ Aby przywrócić ikonę:

- Kliknij przycisk **pokaż**.

Zmiana języka interfejsu

Domyślnie Konsola Rapport i wszystkie pozostałe okna dialogowe są wyświetlane w języku angielskim. Język interfejsu Konsoli Rapport i okien dialogowych można również zmienić na jeden z kilku innych języków.

➔ Aby zmienić język Konsoli Rapport:

1. [Otwórz Konsolę Rapport.](#)
2. W obszarze Ustawienia produktu panelu kontrolnego kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.
3. Z listy **Język** wybierz język. Zostanie wyświetlony następujący komunikat.

Zmiany odniosą skutek w pełni po zamknięciu wszystkich okien przeglądarki.

Przełączyć język i ponownie uruchomić konsolę Trusteer Endpoint Protection?

4. Kliknij przycisk **OK**. Konsola Rapport zostanie ponownie załadowana w wybranym języku.

7. Wyświetlanie informacji o aktywności programu Rapport

Mechanizmy ochrony programu Rapport są aktywowane przez kilka typów zdarzeń. Niektóre z tych zdarzeń to zdarzenia uprawnione, przypominające zdarzenia powodowane przez szkodliwe oprogramowanie. Inne zdarzenia mogą być inicjowane przez szkodliwe oprogramowanie znajdujące się na komputerze. Każde zdarzenie jest zliczane i rejestrowane w raporcie aktywności wyświetlanym w dowolnej chwili. Raport przedstawia aktywność z ostatnich siedmiu dni. Licznik zdarzeń można zresetować lub zatrzymać, albo włączyć lub wyłączyć okno dialogowe z propozycją przedstawienia tygodniowego raportu aktywności, pojawiające się na ekranie na początku każdego tygodnia.

Wyświetlanie raportu o aktywności

Tygodniowy raport o aktywności przedstawia liczbę zdarzeń wyzwolonych przez każdy z mechanizmów ochrony programu Rapport w ciągu ostatnich siedmiu dni. Raport ten służy wyłącznie do celów informacyjnych. Nie jest niezbędne wykonywanie żadnych czynności, ponieważ program Rapport blokuje wszystkie zdarzenia mogące doprowadzić do ujawnienia danych. Raport o aktywności jest wyświetlany automatycznie w ciągu 12 godzin po zainstalowaniu programu Rapport.

Fakt, że raport o aktywności zawiera zdarzenia, nie oznacza jeszcze obecności na komputerze szkodliwego oprogramowania ani faktu odwiedzin oszukańczego serwisu. Oznacza tylko, że oprogramowanie lub odwiedzone serwisy naruszają strategię bezpieczeństwa ustanowioną przez właścicieli chronionych serwisów WWW lub przez IBM. Na przykład możliwe, że używane oprogramowanie próbowało wykonać zrzut ekranu wyciągu bankowego lub odczytać informacje wprowadzone w serwisie WWW bankowości elektronicznej. To naruszenie strategii spowodowało zablokowanie przez program Rapport możliwości dostępu tego oprogramowania do newralgicznych informacji.

➔ Aby w dowolnej chwili wyświetlić tygodniowy raport o aktywności:

1. [Otwórz Konsolę Rapport.](#)
2. W obszarze **Tygodniowy raport o aktywności** panelu kontrolnego kliknij opcję **Pełny raport**. Zostanie wyświetlony Tygodniowy raport o aktywności.

Raport zawiera dziewięć liczników dla dziewięciu kategorii zdarzeń. Kategorie raportu o aktywności zawierają listę różnych typów zdarzeń napotkanych przez program Rapport i zażegnanych podczas przeglądania Internetu.
3. Klikając nazwę każdego licznika, można wyświetlić opis zdarzenia bezpieczeństwa, za którego zliczanie on odpowiada, oraz listę zliczonych zdarzeń danej kategorii.

Uwaga: Nie należy się martwić, jeśli nie wszystkie informacje przedstawione w niniejszym raporcie są jasne, ponieważ ma on charakter nieco specjalistyczny. Przedstawione w nim informacje nie wymagają podjęcia jakichkolwiek czynności przez użytkownika. Raport można bezpiecznie zamknąć i nie trzeba do niego wracać. Jest on zachowywany wyłącznie do wglądu w przyszłości, na potrzeby użytkowników analizujących działanie programu Rapport w dłuższym okresie czasu.

Konfigurowanie raportu o aktywności

Dostępna jest opcja umożliwiająca automatyczne wyświetlanie raportu o aktywności co siedem dni. Raport jest wyświetlany po raz pierwszy automatycznie po upływie 12 godzin od instalacji programu Rapport. Domyślnie raport nie pojawia się co tydzień, lecz można go w dowolnej chwili wyświetlić w Konsoli Rapport.

Wyczyszczenie danych zawartych w tygodniowym raporcie o aktywności powoduje wyzerowanie wszystkich liczników zdarzeń. Wyłączenie tygodniowego raportu o aktywności powoduje zatrzymanie wszystkich liczników zdarzeń.

➔ Aby skonfigurować raport o aktywności:

1. [Otwórz Konsolę Rapport.](#)
2. W obszarze **Tygodniowy raport o aktywności** panelu kontrolnego kliknij opcję **Pełny raport**. Zostanie wyświetlony Tygodniowy raport o aktywności.

Można teraz:

- Włączyć tygodniowy raport o aktywności, zaznaczając pole wyboru **Automatycznie prezentuj ten raport na początku każdego tygodnia**. Co siedem dni będzie wyświetlane okno dialogowe z propozycją wyświetlenia tego raportu.
- [Czyszczenie raportu o aktywności](#).
- [Wyłączanie raportu o aktywności](#).

Czyszczenie raportu o aktywności

➔ Aby wyczyścić raport o aktywności:

1. Kliknij opcję **Wyczyść raport**. Zostanie wyświetlony ekran z potwierdzeniem.
2. Kliknij przycisk **OK**. Wszystkie liczniki zostaną zresetowane.

Wyłączanie raportu o aktywności

➔ Aby wyłączyć tygodniowy raport o aktywności:

1. Kliknij opcję **Wyłącz raport**. Zostanie wyświetlony ekran z potwierdzeniem.
2. Kliknij przycisk **OK**. Liczniki zdarzeń są czyszczone, zaś tygodniowy raport o aktywności jest wyłączany. W obszarze Tygodniowy raport o aktywności panelu kontrolnego jest teraz wyświetlany komunikat „Raport o aktywności jest wyłączony”. Raport można włączyć ponownie, klikając opcję **Włącz raport o aktywności**.

8. Zarządzanie chronionymi serwisami i hasłami

Program Rapport udostępnia informacje dotyczące serwisów WWW i haseł chronionych w Konsoli Rapport. Konsoli Rapport można użyć w celu usunięcia serwisów WWW i haseł.

Istnieją dwie kategorie chronionych serwisów WWW:

- **Zaufane serwisy WWW partnerów.** Są to serwisy WWW należące do partnerów IBM. Zaufani partnerzy współpracują bezpośrednio z IBM w celu zapewnienia optymalnej strategii zabezpieczeń do swoich zastosowań. Uzyskując dostęp do serwisu WWW partnera, użytkownik zyskuje automatyczną ochronę. Nie jest możliwe usunięcie ochrony programem Rapport dla tych serwisów WWW. Liczba chronionych serwisów partnerskich nie powoduje żadnego obciążenia dla systemu.
- **Serwisy WWW dodane ręcznie.** Są to serwisy WWW dodane przez użytkownika ze względu na korzyści płynące z ochrony zapewnianej przez program Rapport podczas nawiązywania z nimi połączenia. Nie obowiązuje żadne ograniczenie co do liczby serwisów, jaką można objąć ochroną. IBM zaleca aktywację ochrony dla programu Rapport we wszystkich dodatkowych serwisach WWW, za pośrednictwem których użytkownik przesyła dane prywatne i osobowe lub wszelkie inne newralgiczne informacje. Przykłady serwisów WWW, których ochrona może być wskazana, to:
 - Rachunki bankowe online
 - Rachunki funduszy inwestycyjnych
 - Rachunki brokerskie online
 - Sklepy internetowe
 - Serwisy e-mail z interfejsem WWW (takie jak Outlook, Yahoo! Mail i Gmail)
 - Serwisy sieci społecznościowych (takie jak Facebook, Orkut czy LinkedIn)
 - Aplikacje ubezpieczeniowe

- Serwisy osobistych informacji medycznych
- Serwisy zakupowe online (takie jak eBay, Amazon, Walmart.com czy Target.com)

Istnieje możliwość usunięcia ochrony przez program Rapport z tych serwisów WWW przez usunięcie ich z listy.

Uwaga: W przypadku niektórych instalacji programu Rapport opcja ręcznego ustawienia ochrony serwisów WWW jest wyłączona.

W obszarze Zaufane serwisy Konsoli Rapport wyświetlana jest liczba serwisów WWW należących do każdej z obecnie chronionych kategorii. Istnieje możliwość wyświetlenia listy i opisu chronionych serwisów WWW naszych partnerów. W tym celu należy kliknąć opcję **Zaufane serwisy WWW partnerów**. Można także wyświetlić listę serwisów WWW dodanych ręcznie przez kliknięcie opcji **Ręcznie dodane serwisy WWW**.

Ochrona dodatkowych serwisów WWW

➔ Aby chronić dodatkowy serwis WWW:

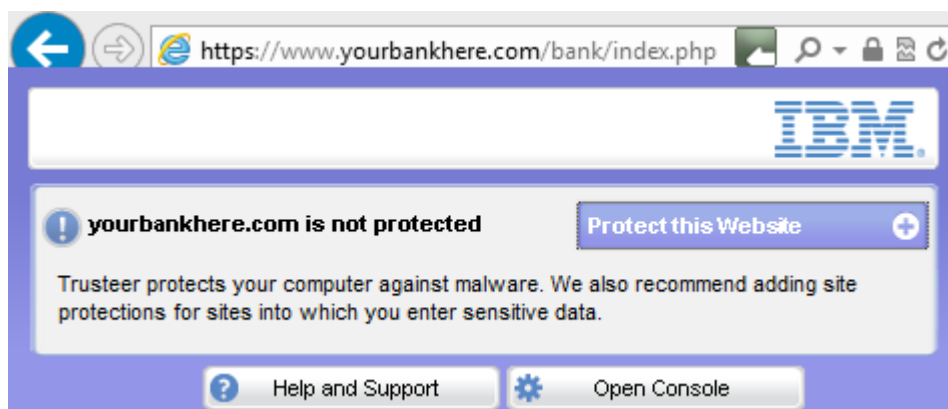
1. Przejdź do serwisu WWW, który chcesz chronić. Jeśli nie włączono jeszcze programu Rapport w celu ochrony tego serwisu WWW, ikona programu Rapport na pasku adresu jest wyszarzona.

Szara ikona Rapport



YourBankHere

2. Kliknij szarą ikonę programu Rapport na pasku adresu. Zostanie wyświetlone okno dialogowe.



3. W oknie dialogowym kliknij opcję **Chroń ten serwis WWW**. Ikona programu Rapport na pasku adresu przyjmuje kolor zielony, co oznacza, że ten serwis WWW jest teraz chroniony przez program Rapport.

Zielona ikona Rapport



YourBankHere

Ikona jest wyświetlana domyślnie. Można również [ukryć ikonę programu Rapport](#).

Dlaczego ikona programu Rapport nie pojawia się w mojej przeglądarce?

Jeśli ikona programu Rapport nie pojawia się w przeglądarce użytkownika, są trzy możliwe przyczyny:

- Wybrano ukrycie ikony na pasku adresu. Program Rapport nadal zapewnia ochronę, lecz ikona nie jest widoczna. Można przywrócić wyświetlanie ikony. Więcej informacji na temat ukrywania i przywracania ikony programu Rapport można znaleźć w sekcji [Ukrywanie i przywracanie ikony programu Rapport na pasku adresu](#).

- Program Rapport nie obsługuje przeglądarki użytkownika. Listę obecnie obsługiwanych przeglądarek można znaleźć pod adresem:
<http://www.trusteer.com/support/supported-platforms>.
- Program Rapport został zatrzymany i nie działa. Można uruchomić program Rapport ponownie. Więcej informacji można znaleźć w sekcji [Uruchamianie programu Rapport](#).

Usuwanie chronionych serwisów WWW

➔ Aby usunąć ręcznie dodane serwisy WWW:

1. [Otwórz Konsole Rapport](#).
2. W obszarze Zaufane serwisy WWW kliknij opcję **Przeglądaj zaufane serwisy WWW**. Zostanie wyświetlona karta Zaufane serwisy WWW.
3. Kliknij opcję **Serwisy WWW dodane ręcznie**. Zostanie wyświetlona lista wszystkich ręcznie dodanych serwisów WWW.
4. Kliknij odsyłacz **usuń** obok serwisu WWW na tej liście. Zostanie wyświetlony ekran z potwierdzeniem.
5. Kliknij przycisk **OK**. Serwis WWW zostanie usunięty z listy. Ikona programu Rapport będzie teraz wyszarzona po przejściu do usuniętego serwisu WWW, co będzie oznaczać, że nie jest on już chroniony.

Zarządzanie chronionymi nazwami użytkowników i hasłami

Po zaakceptowaniu propozycji programu Rapport ochrony hasła w chronionym serwisie nie tylko zapewnia on ochronę hasła, lecz także chroni wszelkie przyszłe hasła wprowadzane w tej witrynie. Program Rapport zapamiętuje wybór użytkownika o ochronie hasła lub jej braku dla każdego serwisu. Nie oferuje on ponownej ochrony hasła po przejściu do tego serwisu, o ile użytkownik nie wyczyści pamięci podręcznej ochrony haseł. Konsola Rapport wskazuje, dla których serwisów WWW jest obecnie włączona ochrona haseł programu Rapport. W razie potrzeby możliwe jest wyłączenie ochrony hasła dla dowolnego chronionego serwisu WWW. Można także wyczyścić pamięć podręczną ochrony hasła, powodującą skasowanie wszystkich mechanizmów ochrony haseł i decyzji o ochronie haseł.

Uwaga: W przypadku niektórych serwisów WWW partnerów IBM program Rapport chroni nie tylko hasła, ale i nazwy użytkowników. Konsola Rapport wskazuje także strategię ochrony nazwy użytkownika dla serwisu WWW.

➔ Aby wyłączyć ochronę hasła dla chronionego serwisu WWW:

1. [Otwórz Konsolę Rapport.](#)
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Przewiń w dół listy mechanizmów zabezpieczeń, aż do odnalezienia opcji **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**.

6. Kliknij opcję **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**. Wyświetlona zostanie strategia zabezpieczeń nazw użytkowników i haseł dla każdego serwisu WWW.
7. Usuń zaznaczenie pola wyboru **Ostrzegaj w przypadku użycia hasła w innym miejscu** dla serwisu WWW, dla którego ma zostać wyłączona ochrona hasła. Program Rapport nie będzie zapewniał ochrony hasła tego serwisu WWW.

Uwaga: Kliknięcie opcji **Wyczyść pamięć podręczną** powoduje wyczyszczenie wszystkich ustawień ochrony hasła i zresetowanie wszystkich strategii ochrony hasła, co spowoduje ponowne wyświetlenie w programie Rapport oferty ochrony hasła przy kolejnej wizycie w każdym z serwisów WWW.

8. Kliknij przycisk **Zapisz**. Zmiany zostaną zapisane.

9. Rozwiązywanie problemów

Problem z programem Rapport? Pod adresem <http://www.trusteer.com/support/faq> można znaleźć listę często zadawanych pytań dotyczących rozwiązywania problemów.

Aby dowiedzieć się, jak można uzyskać wsparcie, należy zapoznać się z punktem [Uzyskiwanie wsparcia](#). W poniższych sekcjach można znaleźć informacje o tym, jak wykonać niektóre procedury niezbędne przy rozwiązywaniu problemów.

Uwaga: Zawsze istnieje możliwość [wyłączenia programu Rapport](#) bez konieczności usuwania programu Rapport z komputera, w celu sprawdzenia, czy dany problem dotyczy programu Rapport. Należy unikać usuwania programu Rapport podczas rozwiązywania problemów. [Zatrzymanie programu Rapport](#) ma ten sam skutek i umożliwia IBM szybkie i efektywne rozwiązanie problemów podczas kontaktu z działem wsparcia.

Zatrzymywanie programu Rapport

Zatrzymanie programu Rapport powoduje szybkie i proste zatrzymanie funkcji programu bez jego deinstalowania. Program Rapport można zatrzymać w celu sprawdzenia, czy jest on przyczyną doświadczanych problemów. W celu ponownego uruchomienia programu Rapport należy [uruchomić program Rapport](#). Nie ma potrzeby jego reinstalowania.

W przypadku wystąpienia problemu i podejrzenia, że jego przyczyną może być program Rapport, należy spróbować zatrzymać program Rapport. Jeśli problem nie ustąpi mimo zatrzymania programu Rapport, oznacza to, że prawdopodobieństwo, iż to program Rapport jest przyczyną problemu, jest nikłe. Jeśli problem zniknie po zatrzymaniu programu Rapport, oznacza to, że program Rapport jest prawdopodobnie przynajmniej w części przyczyną problemu.

IBM nie zaleca deinstalowania programu Rapport. Przed podjęciem ostatecznej decyzji o deinstalacji programu Rapport należy skontaktować się z działem wsparcia IBM Trusteer w celu uzyskania pomocy. Więcej informacji można znaleźć w punkcie [Uzyskiwanie wsparcia](#).

Uwaga: Jeśli program Rapport zainstalowano z konta administratora systemu Windows, wówczas można zatrzymać program Rapport wyłącznie po zalogowaniu się z konta administratora.

➔ **Aby zatrzymać program Rapport:**

1. Zapisz dane i zamknij wszystkie otwarte okna.

Uwaga: Nie zatrzymuj programu Rapport, jeśli otwarte jest okno przeglądarki. Zatrzymanie programu Rapport przy otwartym oknie przeglądarki może spowodować awarię.

2. Z menu Start systemu Windows wybierz opcje **Programy > Trusteer Endpoint Protection > Zatrzymaj program Trusteer Endpoint Protection**. Zostanie wyświetlony komunikat zabezpieczający z prośbą o potwierdzenie. Wraz z komunikatem wyświetlany jest obrazek zawierający kilka znaków do przepisania. Ma to na celu zabezpieczenie przed wyłączeniem programu Rapport przez szkodliwe oprogramowanie.
3. Wprowadź znaki widoczne na obrazku.
4. Kliknij opcję **Zamknij**. Podczas zamykania programu Rapport wyświetlany jest następujący komunikat: „Należy poczekać na zamknięcie programu Trusteer Endpoint Protection.” Zniknięcie tego komunikatu oznacza, że działanie programu Rapport zostało przerwane. Można także dodatkowo sprawdzić, że program Rapport nie działa. W tym celu należy otworzyć okno przeglądarki i upewnić się, że ikona programu Rapport nie jest wyświetlana po prawej stronie paska adresu.

Uruchamianie programu Rapport

Uruchomienie programu Rapport powoduje wznowienie jego pracy, jeśli wcześniej został on zatrzymany.

Uwaga: Jeśli program Rapport zainstalowano z konta administratora systemu Windows, wówczas można uruchomić program Rapport wyłącznie po zalogowaniu się z konta administratora.

➔ Aby uruchomić program Rapport:

Z menu Start wybierz opcje **Programy > Trusteer Endpoint Protection > Uruchom program Trusteer Endpoint Protection**. Zostanie wyświetlony komunikat „Należy poczekać na uruchomienie programu Trusteer Endpoint Protection”. Zniknięcie tego komunikatu oznacza, że program Rapport został ponownie uruchomiony. Można sprawdzić, czy program Rapport działa, sprawdzając ikonę programu Rapport na pasku zadań ().

Uzyskiwanie wsparcia

Usługi wsparcia dla programu IBM Trusteer są stale dostępne. IBM oferuje szereg opcji wsparcia:

- Jeśli na komputerze zainstalowano program Rapport i nie występują problemy z nawiązywaniem połączeń, można rozpocząć zgłaszanie problemu za pośrednictwem Konsoli Rapport. Zobacz punkt [Wysyłanie raportu dotyczącego problemu użytkownika](#). Po zgłoszeniu problemu za pośrednictwem Konsoli Rapport program Rapport przesyła do IBM wniosek o wsparcie z raportem dotyczącym problemu oraz ważne pliki dzienników ułatwiające IBM znalezienie rozwiązania problemu.
- Jeśli program Rapport nie jest zainstalowany lub jeśli nie można przestać za jego pośrednictwem wniosku o wsparcie, należy skorzystać z formularza na stronie <http://www.trusteer.com/support/submit-ticket>. Należy uwzględnić możliwie najwięcej informacji zarówno na temat problemu, jak i komputera, w tym systemu operacyjnego, przeglądarki, zaobserwowanego działania oraz inne stosowne szczegółowe dane.
- W przypadku napotkania problemów z wydajnością, połączeniem, stabilnością lub innych problemów dotyczących przeglądarki należy kliknąć odsyłacz „Live Support” dostępny pod adresem <http://www.trusteer.com/support> w celu uruchomienia czatu online z przedstawicielem działu wsparcia.

Uwaga: W przypadku pytań dotyczących programu Rapport, jeśli nie występuje żaden konkretny problem, należy przeszukać niniejszy podręcznik lub skorzystać z usługi Błyskawiczne odpowiedzi na stronie WWW: <http://www.trusteer.com/support/faq>.

Odblokowywanie uprawnionych programów dodatkowych przeglądarki

Jeśli niektóre strony WWW nie są wyświetlane prawidłowo i zachodzi podejrzenie, że uprawniony program dodatkowy może być blokowany, można sprawdzić, czy program Rapport nie blokuje tego programu dodatkowego.

➔ Aby odblokować uprawniony program dodatkowy w przeglądarce:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Blokuj nieznane programy dodatkowe w przeglądarce**. Zostanie wyświetlona lista zablokowanych programów dodatkowych. Obok nazwy każdego z zablokowanych programów dodatkowych znajduje się pole wyboru **Zawsze zezwalaj na działanie tego programu dodatkowego**.
6. Zaznacz pole wyboru **Zawsze zezwalaj na działanie tego programu dodatkowego** dla zablokowanego programu dodatkowego, na którego działanie chcesz zezwolić.

7. Kliknij przycisk **Zapisz**. Program dodatkowy jest teraz odblokowany.

Wyłączanie blokady rejestrowania naciśnień klawiszy

Funkcja blokowania rejestrowania naciśnień klawiszy programu Rapport może kolidować z innymi programami do rejestracji naciśnień klawiszy i generować nieprawidłowe naciśnięcia klawiszy. Stąd, jeśli na komputerze działa inny program blokujący rejestrację naciśnień klawiszy (na przykład stanowiący składnik oprogramowania antywirusowego), może zaistnieć potrzeba wyłączenia tej funkcji. Alternatywnie można także wyłączyć aktywny program blokujący rejestrację naciśnień klawiszy.

➔ Aby wyłączyć funkcję blokowania rejestracji naciśnień klawiszy:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Z listy obok pola **Aktywuj zastępowanie znaków** wybierz opcję **Nigdy**. Zostanie wyświetlony następujący komunikat:

Po ustawieniu dla opcji Aktywuj zastępowanie znaków wartości Nigdy program Trusteer Endpoint Protection nie chroni kart płatniczych. Można przywrócić wartości domyślne, włączyć zastępowanie znaków albo wyłączyć ochronę kart płatniczych tak, aby ustawienia były spójne.

6. Kliknij przycisk **OK**.
7. Z listy obok pola **Aktywuj zastępowanie znaków na poziomie jądra** wybierz opcję **Nigdy**.
8. Kliknij przycisk **Zapisz**. Zostanie wyświetlony komunikat z informacją, że zmiany odniosą skutek po zrestartowaniu komputera.
9. Kliknij przycisk **OK**.
10. Zrestartuj komputer. Funkcja blokowania rejestrowania naciśnieć klawiszy programu Rapport jest wyłączona.

Cofanie przypadkowych autoryzacji

W przypadku niektórych ostrzeżeń programu Rapport możliwa jest autoryzacja serwisów WWW lub certyfikatów nierozpoznawanych przez program Rapport jako uprawnione. Po dokonaniu autoryzacji serwisu WWW lub certyfikatu użytkownik nie jest ponownie ostrzegany w przypadku tego samego serwisu WWW lub certyfikatu, ponieważ jest on już zapisany w pamięci podręcznej. W razie przypadkowej autoryzacji serwisu WWW lub certyfikatu istnieje możliwość wyczyszczenia pamięci podręcznej, tak że ten sam serwis lub certyfikat spowoduje wygenerowanie ostrzeżenia przy ponownej próbie nawiązania połączenia.

Usuwanie autoryzowanych nieważnych certyfikatów SSL

Po wykryciu przez program Rapport, że [certyfikat³](#) serwisu WWW jest niepoprawny program Rapport wyświetla [Ostrzeżenie o nieważności certyfikatu](#), aby ostrzec użytkownika przed wysłaniem newralgicznych danych do oszukańczych serwisów WWW. Po zaznaczeniu opcji **Nie wyświetlaj ostrzeżenia dotyczącego tego serwisu WWW ponownie** w oknie dialogowym Ostrzeżenie o nieważnym certyfikacie certyfikat serwisu WWW, z którym nawiązywane jest połączenie, jest dodawany do pamięci podręcznej zawierającej autoryzowane nieważne certyfikaty. Wyczyszczenie pamięci podręcznej powoduje usunięcie autoryzacji dla wszelkich certyfikatów znajdujących się w pamięci podręcznej i powoduje, że program Rapport ostrzega użytkownika ponownie podczas próby ponownych odwiedzin w tych samych serwisach WWW.

➔ Aby skasować autoryzowane nieważne certyfikaty SSL:

1. [Otwórz Konsole Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

³ Certyfikat SSL to kryptograficzny certyfikat cyfrowy potwierdzający tożsamość serwisu WWW i tworzący zaszyfrowane połączenie umożliwiające przesyłanie newralgicznych danych do serwisu WWW. Symbol kłódki na pasku adresu przeglądarki lub w dolnej części przeglądarki oznacza, że połączenie między przeglądarką a serwisem WWW jest zabezpieczone protokołem SSL. Jednocześnie jednak obecność symbolu kłódki nie gwarantuje, że certyfikat jest poprawny.

5. Kliknij opcję **Sprawdź poprawność certyfikatów SSL serwisu WWW**.
Informacje o tym mechanizmie pojawią się poniżej, wraz z odsyłaczem umożliwiającym **wyczyszczenie pamięci podręcznej**.
6. Kliknij opcję **Wyczyść pamięć podręczną** po rozwinięciu bloku informacji.
Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**. Pamięć podręczna zostanie wyczyszczona.

Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych kart płatniczych

Po wykryciu przez program Rapport faktu wprowadzenia numeru karty płatniczej na stronie WWW na dysku lokalnym lub w dowolnym niezabezpieczonym serwisie WWW program Rapport wyświetli [ostrzeżenie o wykryciu operacji przesyłania karty płatniczej](#). Ten komunikat jest wyświetlany, aby zapobiec przesłaniu numeru karty płatniczej do serwisu WWW wyludzającego informacje lub do serwisu uprawnionego, lecz nie zapewniającego odpowiedniego poziomu bezpieczeństwa. Kliknięcie opcji **Ignoruj, ten serwis WWW jest zaufany** w oknie dialogowym ostrzeżenia o wykryciu próby wprowadzenia danych karty płatniczej serwis WWW jest dodawany do listy serwisów wybranych jako zaufane i użytkownik nie jest ponownie ostrzegany przy wprowadzaniu numeru karty płatniczej do tego serwisu. Można usunąć serwis z tej listy.

➔ Aby usunąć serwisy wybrane jako zaufane na potrzeby wprowadzania danych kart płatniczych:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.

3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij opcję **Chroń numery kart płatniczych przed kradzieżą**. Wszystkie serwisy wybrane jako zaufane są wymienione na liście w rozwijanym obszarze. W rozwijanym obszarze znajduje się lista serwisów, które wybrano jako zaufane przez kliknięcie opcji **Ignoruj, ten serwis jest zaufany** w oknie dialogowym ostrzeżenia o wykryciu operacji wprowadzania danych karty płatniczej.
6. Kliknij opcję **Usuń ten serwis** dla każdego serwisu, który chcesz usunąć z listy, lub kliknij opcję **Usuń wszystkie serwisy**, aby usunąć wszystkie zaufane serwisy. Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**.

Usuwanie serwisu z listy zaufanych na potrzeby wprowadzania danych bez zabezpieczenia

Po wykryciu przez program Rapport faktu wprowadzenia hasła do serwisu WWW, który nie przesyła danych w sposób bezpieczny, program Rapport wyświetla [ostrzeżenie dotyczące wprowadzania danych bez zabezpieczenia](#). Jest ono wyświetlane, aby ostrzec użytkownika przed wprowadzaniem newralgicznych danych do serwisów o wysokim stopniu ryzyka, w tym do serwisów uprawnionych, które mogą łatwo zostać przejęte przez grupy przestępcze.

Kliknięcie opcji **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie** w tym oknie dialogowym powoduje, że serwis WWW jest dodawany do listy serwisów WWW wybranych jako zaufane i użytkownik nie jest ostrzegany ponownie w przypadku wprowadzenia numeru karty płatniczej do tego serwisu. Można usunąć serwis z tej listy.

➔ Aby usunąć niezabezpieczone serwisy WWW wybrane wcześniej jako zaufane:

1. [Otwórz Konsolę Rapport.](#)
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.
5. Kliknij element **Ostrzegaj, kiedy przesyłam zabezpieczone dane do niezabezpieczonych serwisów**. Wszystkie serwisy wybrane jako zaufane są wymienione na liście w rozwijanym obszarze. W rozwijanym obszarze wyświetlane są serwisy, które wybrano jako zaufane, klikając opcję **Ten serwis jest zaufany, nie wyświetlaj alertu ponownie** w oknie dialogowym [ostrzeżenia o wykryciu operacji wprowadzania danych bez zabezpieczenia](#) lub klikając opcję **Ten serwis jest zaufany** w oknie dialogowym [ostrzeżenia o ochronie informacji](#).
6. Kliknij opcję **Usuń ten serwis** dla każdego serwisu, który chcesz usunąć z listy, lub kliknij opcję **Usuń wszystkie serwisy**, aby usunąć wszystkie zaufane serwisy. Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**.

Usuwanie serwisów WWW, dla których zezwolono na wysyłanie danych logowania

Po wprowadzeniu tekstu zgodnego z chronionym hasłem do nieznanego serwisu WWW w programie Rapport wyświetlane jest [Ostrzeżenie dotyczące danych chronionych](#). Jeśli wybrano ignorowanie tego ostrzeżenia, serwis staje się serwisem autoryzowanym i program Rapport nie ostrzega użytkownika przy wprowadzaniu chronionego hasła do tego serwisu WWW. Autoryzowane w ten sposób serwisy WWW są przechowywane w pamięci podręcznej. Wyczyszczenie pamięci podręcznej powoduje usunięcie takich wcześniej dokonanych autoryzacji.

Po przypadkowym kliknięciu opcji **Ignoruj to ostrzeżenie** w oknie dialogowym Ostrzeżenie o danych chronionych może okazać się potrzebne skasowanie autoryzowanych serwisów WWW zapisanych w pamięci podręcznej, do których zezwolono na wysyłanie danych logowania. Wyczyszczenie pamięci podręcznej nie powoduje cofnięcia operacji przesyłania hasła, które miały już miejsce, lecz powoduje zresetowanie nieznanego statusu serwisów WWW, które zostały przypadkowo autoryzowane.

➔ Aby wyczyścić pamięć podręczną autoryzowanych serwisów WWW, dla których zezwolono na wysyłanie danych logowania:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Strategia bezpieczeństwa kliknij opcję **Edytuj strategię**. Zostanie wyświetlony ekran Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek ze słowem, które należy wpisać, aby uniemożliwić dostęp do konsoli i wyłączenie programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.

Kliknij przycisk **OK**. Zostanie wyświetlony ekran Strategia bezpieczeństwa, zawierający wszystkie mechanizmy zabezpieczeń.

5. Przewiń w dół do pozycji **Ostrzegaj, kiedy dane logowania zostaną użyte w nieznanych serwisach WWW**, a następnie kliknij nazwę mechanizmu. Informacje o tym mechanizmie pojawią się poniżej, wraz z odsyłaczem umożliwiającym **wyczyszczenie pamięci podręcznej**.
6. Kliknij opcję **Wyczyść pamięć podręczną** po rozwinięciu bloku informacji. Zostanie wyświetlony ekran z potwierdzeniem.
7. Kliknij przycisk **OK**. Pamięć podręczna zostanie wyczyszczona.

Postępowanie w przypadku błędów

Po wyświetleniu błędu programu Rapport, jeśli potrzebne są pewne informacje na jego temat, należy zapoznać się z poniższymi informacjami.

Postępowanie w przypadku błędów aktualizacji

Poniższy tekst stanowi przykład błędu dotyczącego aktualizacji programu Rapport:

*Program Trusteer Endpoint Protection nie mógł odebrać aktualizacji.
Kliknij przycisk OK, aby skonfigurować nazwę użytkownika i hasło serwera proxy.*

Ten błąd występuje, jeśli program Rapport nie mógł nawiązać połączenia z Internetem w celu sprawdzenia dostępności aktualizacji. Ten błąd może wystąpić w przypadku nawiązania połączenia z siecią Internet za pośrednictwem serwera proxy, gdy program Rapport nie mógł automatycznie wykryć szczegółowych danych serwera proxy.

➔ W przypadku odebrania tego błędu:

1. Kliknij przycisk **OK**. Zostanie otwarta Konsola Rapport z kartą Połączenie internetowe.
2. Wybierz opcję **Użyj serwera proxy**. Wprowadź w podanym polu nazwę serwera proxy lub adres IP.

3. W polu **Port** wprowadź port TCP, który ma być używany do nawiązania połączenia z serwerem proxy.
4. Jeśli serwer proxy użytkownika wymaga uwierzytelnienia, wprowadź nazwę użytkownika w polu **Nazwa użytkownika serwera proxy** i hasło w polu **Hasło serwera proxy**.
5. Kliknij opcję **Zastosuj ustawienia**.
6. Kliknij opcję **Sprawdź połączenie**, aby po skonfigurowaniu serwera proxy sprawdzić, czy program Rapport ma połączenie z Internetem.

Postępowanie w przypadku błędów instalatora programu Rapport

Proces instalowania programu Rapport przebiega dwustopniowo:

1. Użytkownik pobiera plik RapportSetup.exe (plik programu startowego).
2. Po uruchomieniu tego pliku przez użytkownika pobierany jest plik instalacji pełnej. Jeśli proces pobierania nie powiedzie się, co zdarza się niekiedy w przypadku obecności firewalla blokującego pobieranie, może zostać wyświetlony komunikat o błędzie „Błąd podczas wyodrębniania pakietu konfiguracji programu Rapport”.

Aby rozwiązać ten problem, należy pobrać pełny pakiet konfiguracyjny z następującego serwisu WWW: <http://www.trusteer.com/support/install-troubleshooting>.

Poniższy tekst stanowi przykład błędu dotyczącego instalowania programu Rapport:

Niestety pobranie pakietu programu instalacyjnego nie było możliwe. Kliknij przycisk „OK”, aby zamknąć okno konfiguracji. Nastąpi automatyczne przejście do strony pobierania, na której można bezpośrednio pobrać pakiet programu instalacyjnego i zainstalować go. Jeśli problem nie ustąpi, należy sprawdzić ustawienia sieciowe i firewall.

Ten błąd pojawia się podczas instalacji programu Rapport, jeśli instalator programu Rapport nie mógł pobrać pełnego pakietu programu instalacyjnego.

W przypadku wyświetlenia tego błędu kliknij przycisk **OK**. Zostanie wyświetlony serwis WWW IBM. Pełny pakiet programu instalacyjnego można pobrać z serwisu WWW:

<http://www.trusteer.com/support/install-troubleshooting>.

Uwaga: Jeśli instrukcje dostępne w serwisie WWW nie okażą się pomocne, należy skorzystać z usług wsparcia dla programu IBM Trusteer pod adresem <http://www.trusteer.com/support/submit-ticket>.

Postępowanie w przypadku błędów dotyczących deinstalacji

Poniższy tekst stanowi przykład błędu, jaki może wystąpić podczas procesu deinstalowania:

Niektóre z plików programu Trusteer Endpoint Protection są zablokowane przez inne oprogramowanie. Jeśli przeglądarka jest otwarta, należy ją zamknąć, a następnie podjąć próbę zdeinstalowania programu Trusteer Endpoint Protection. Jeśli problem nie ustąpi, należy zapoznać się z treścią serwisu http://rapport.trusteer.com/installer/troubleshoot_uninstall

Ten komunikat pojawia się w przypadku zablokowania któregośkolwiek z plików programu Rapport przez inny program podczas próby zdeinstalowania programu Rapport.

W przypadku wyświetlenia tego błędu należy postępować zgodnie z instrukcjami podanymi w oknie dialogowym. Istnieje także możliwość pobrania narzędzia Safe Uninstall, którego można użyć do zdeinstalowania programu Rapport; narzędzie można pobrać w serwisie WWW: <http://www.trusteer.com/support/uninstall-troubleshooting>.

Uwaga: Jeśli instrukcje zamieszczone w serwisie WWW nie okażą się pomocne, należy przesłać odpowiednie zgłoszenie do działu wsparcia (adres: <http://www.trusteer.com/support/submit-ticket>).

Konfigurowanie serwera proxy na potrzeby automatycznych aktualizacji

Program Rapport automatycznie łączy się z Internetem w celu sprawdzenia dostępności aktualizacji i pobrania strategii bezpieczeństwa. Większość konfiguracji serwera proxy jest wykrywana automatycznie przez program Rapport bez dokonywania jakichkolwiek zmian w konfiguracji. Jednak, jeśli z nieznanego powodu program Rapport nie może automatycznie wykryć serwera proxy, konieczna jest jego konfiguracja.

➔ Aby skonfigurować serwer proxy:

1. [Otwórz Konsolę Rapport](#).
2. W panelu kontrolnym kliknij opcję . Zostanie wyświetlony dodatkowy panel kontrolny.
3. W obszarze Wydajność i połączenia, obok pola Połączenie internetowe, kliknij opcję **Zmień**. Zostanie wyświetlona karta Połączenie internetowe.
4. Wybierz opcję **Użyj serwera proxy**. Wprowadź w podanym polu nazwę serwera proxy lub adres IP.
5. W polu **Port** wprowadź port TCP, który ma być używany do nawiązania połączenia z serwerem proxy.
6. Jeśli serwer proxy użytkownika wymaga uwierzytelnienia, wprowadź nazwę użytkownika w polu **Nazwa użytkownika serwera proxy** i hasło w polu **Hasło serwera proxy**.
7. Kliknij opcję **Zastosuj ustawienia**.
8. Kliknij opcję **Sprawdź połączenie**, aby po skonfigurowaniu serwera proxy sprawdzić, czy program Rapport ma połączenie z Internetem.

Wysyłanie przez użytkownika raportu o problemie

W przypadku korzystania przez użytkownika z funkcji raportowania problemów dotyczących programu Rapport wysyła on raport techniczny zawierający ważne pliki wewnętrzne dzienników programu Rapport wraz z opisem problemu. Ten raport techniczny może pomóc IBM w identyfikacji i rozwiązywaniu problemów. Jest to najlepszy sposób zgłaszania problemów, ponieważ daje on IBM wyczerpujące informacje dotyczące problemu użytkownika, ułatwiające IBM zapewnienie mu optymalnego wsparcia.

Uwaga: Informacje zawarte w plikach dzienników to dane techniczne, niezawierające informacji newralgicznych ani osobistych.

➔ Aby zgłosić problem:

1. [Otwórz Konsolę Rapport](#). Zostanie wyświetlony panel kontrolny.
2. W obszarze Pomoc i wsparcie kliknij opcję **Zgłoś problem**. Zostanie wyświetlona karta Zgłoś problem.
3. W polu **Imię i nazwisko** opcjonalnie wprowadź swoje imię i nazwisko.
4. W polu **Adres e-mail** wprowadź swój adres e-mail. IBM prześle na ten adres rozwiązanie zgłoszonego problemu.
5. W polu **Opis problemu** wprowadź pełny opis problemu. Podaj możliwie dokładne dane.
6. Kliknij przycisk **Prześlij**. Podczas przesyłania raportu o problemie przez program Rapport w prawym dolnym rogu ekranu wyświetlany jest poniższy komunikat.

Program Trusteer Endpoint Protection wysyła raport o problemie...

Po wysłaniu raportu wyświetlany jest komunikat z potwierdzeniem, że raport został przesłany.

Ostatni wniosek o wsparcie został pomyślnie przesłany do programu Trusteer.

Przedstawiciel IBM skontaktuje się z użytkownikiem za pośrednictwem poczty elektronicznej w celu udzielenia pomocy w rozwiązaniu tego problemu.

Kopiowanie identyfikatora programu Trusteer Endpoint Protection

W przypadku zwrócenia się o pomoc do działu wsparcia dla programu IBM Trusteer może okazać się konieczne podanie numeru identyfikatora programu Trusteer Endpoint Protection. Numer identyfikatora programu Trusteer Endpoint Protection można skopiować z obszaru Ustawienia produktu w Konsoli.

➔ Aby skopiować identyfikator programu Trusteer Endpoint Protection:

1. [Otwórz Konsolę Rapport](#). Zostanie wyświetlony panel kontrolny.
2. W obszarze Ustawienia produktu kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.
3. Kliknij opcję **Kopiuj identyfikator Trusteer Endpoint Protection**. Identyfikator programu Trusteer Endpoint Protection zostanie zapisany w schowku na komputerze.
4. W oknie wiadomości e-mail naciśnij kombinację klawiszy Ctrl+V, aby wkleić identyfikator programu Trusteer Endpoint Protection do swojej wiadomości e-mail.

Wysyłanie plików dzienników programu Rapport do IBM

Jeśli pracownik działu wsparcia dla programu IBM Trusteer poprosi o odszukanie na komputerze plików dzienników programu Rapport i wysłanie ich do IBM w celu ułatwienia rozwiązania problemu, użytkownik powinien wykonać procedurę podaną na stronie WWW: <http://www.trusteer.com/support/gathering-rapport-logs>.

10. Aktualizowanie programu Rapport

Regularne aktualizacje mają kluczowe znaczenie dla skuteczności działania programu Rapport. Z tego względu aktualizacje programu Rapport są wykonywane automatycznie. Aktualizacje pojawiają się niezależnie i bez wiedzy użytkownika. Można jednak zaktualizować program Rapport ręcznie odpowiednio do potrzeb oraz wyłączyć automatyczne aktualizacje.

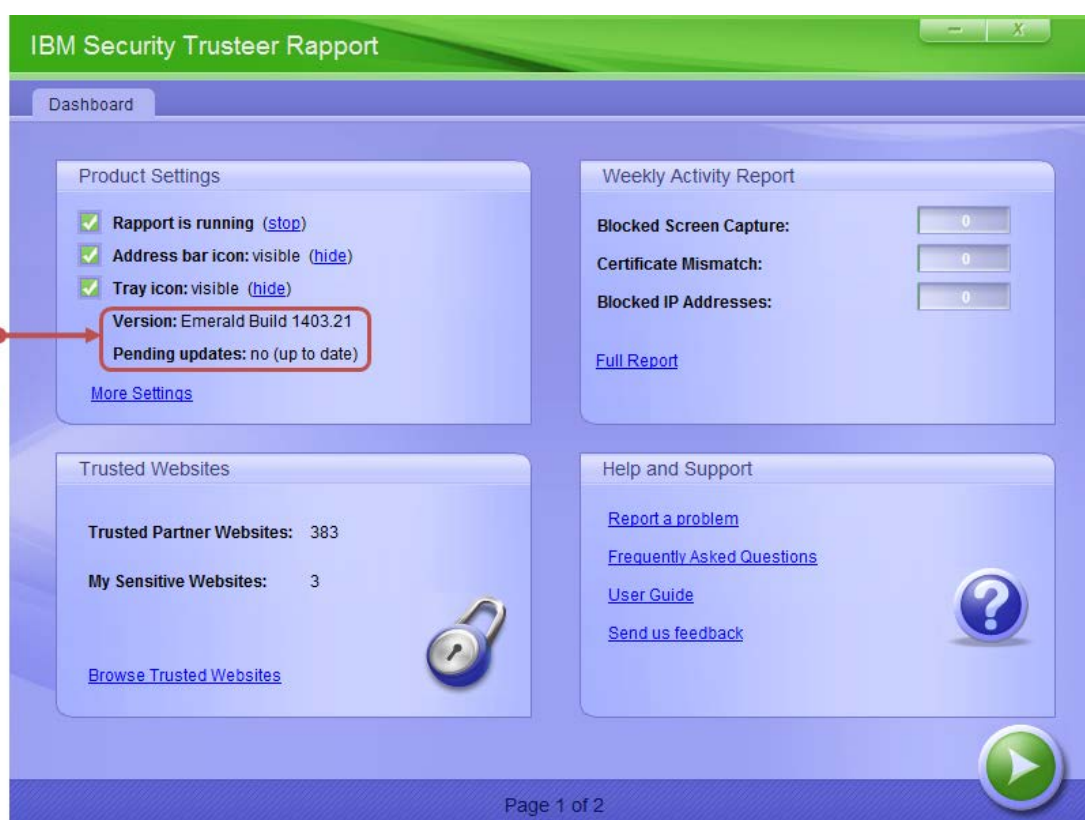
Sprawdzanie statusu aktualizacji programu Rapport

Informacje związane ze statusem aktualizacji programu Rapport są wyświetlane w obszarze Ustawienia produktu Konsoli Rapport.

➔ Aby sprawdzić status aktualizacji programu Rapport:

1. [Otwórz Konsolę Rapport](#). Obszar Ustawienia produktu zostanie wyświetlony w górnym lewym rogu panelu kontrolnego.

Informacje o wersji i aktualizacjach



Pole **Oczekujące aktualizacje** informuje użytkownika o dostępności oczekujących aktualizacji oraz o tym, czy wersja programu Rapport jest aktualna. Jeśli ostatnia pobrana aktualizacja wymaga zrestartowania systemu, aby możliwe było jej zastosowanie, w tym polu wyświetlana jest wartość *tak*.

2. Opcjonalnie kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu, zawierająca dodatkowe informacje.

Poniższe pola wyświetlania podlegają aktualizacji:

- **Ostatnie zapytanie o aktualizacje.** Data i godzina ostatniego przesłania przez program Rapport zapytania o nowe aktualizacje.
- **Automatyczne aktualizacje oprogramowania.** Informacja o tym, czy automatyczne aktualizacje są włączone, czy wyłączone. Domyślnie aktualizacje są włączone. Aby mieć pewność co do otrzymywania wszystkich aktualizacji, należy pozostawić dla tego ustawienia wartość domyślną.

Ręczne aktualizowanie programu Rapport

Program Rapport jest domyślnie aktualizowany automatycznie. Można także zaktualizować program Rapport ręcznie.

➔ Aby ręcznie zaktualizować program Rapport:

1. [Otwórz Konsołę Rapport](#). Obszar Ustawienia produktu zostanie wyświetlony w górnym lewym rogu panelu kontrolnego.



2. Kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.
3. Kliknij opcję **sprawdź teraz w poszukiwaniu aktualizacji**. Program Rapport dokonuje sprawdzenia w poszukiwaniu aktualizacji. Kiedy program Rapport sprawdza dostępność aktualizacji, postęp jest wskazywany przez tekst pojawiający się poniżej pól wyświetlania. Poniższa lista zawiera opis możliwych wyników sprawdzania w poszukiwaniu aktualizacji:

- Program Rapport nie wykrywa oczekujących aktualizacji. Wyświetlany jest komunikat: „Najnowsza konfiguracja programu Rapport została już uruchomiona.”
- Program Rapport wykrywa i pobiera, a następnie instaluje aktualizację. Wyświetlany jest komunikat: „Konfiguracja została zaktualizowana. Uruchomiona jest teraz najnowsza wersja konfiguracji programu Rapport.” Liczba w polu wyświetlania **Plik konfiguracyjny** jest zwiększana.
- Program Rapport wykrywa i pobiera aktualizację, która ma zostać zastosowana przy ponownym uruchomieniu komputera. Wyświetlany jest następujący komunikat: „Aktualizacja oprogramowania jest gotowa. Konfiguracja została zaktualizowana.” Wartość w polu **Oczekujące aktualizacje** zmienia się na „tak (aby zastosować, zrestartuj komputer)”.
- Program Rapport wykrywa i pobiera więcej niż jedną aktualizację. Niektóre aktualizacje są stosowane niezwłocznie, inne zaś zostaną zastosowane po zrestartowaniu komputera. Wyświetlany jest następujący komunikat: „Aktualizacja oprogramowania jest gotowa. Konfiguracja została zaktualizowana.” Liczba w polu wyświetlania **Plik konfiguracyjny** jest zwiększana. Wartość w polu **Oczekujące aktualizacje** zmienia się na „tak (aby zastosować, zrestartuj komputer)”.

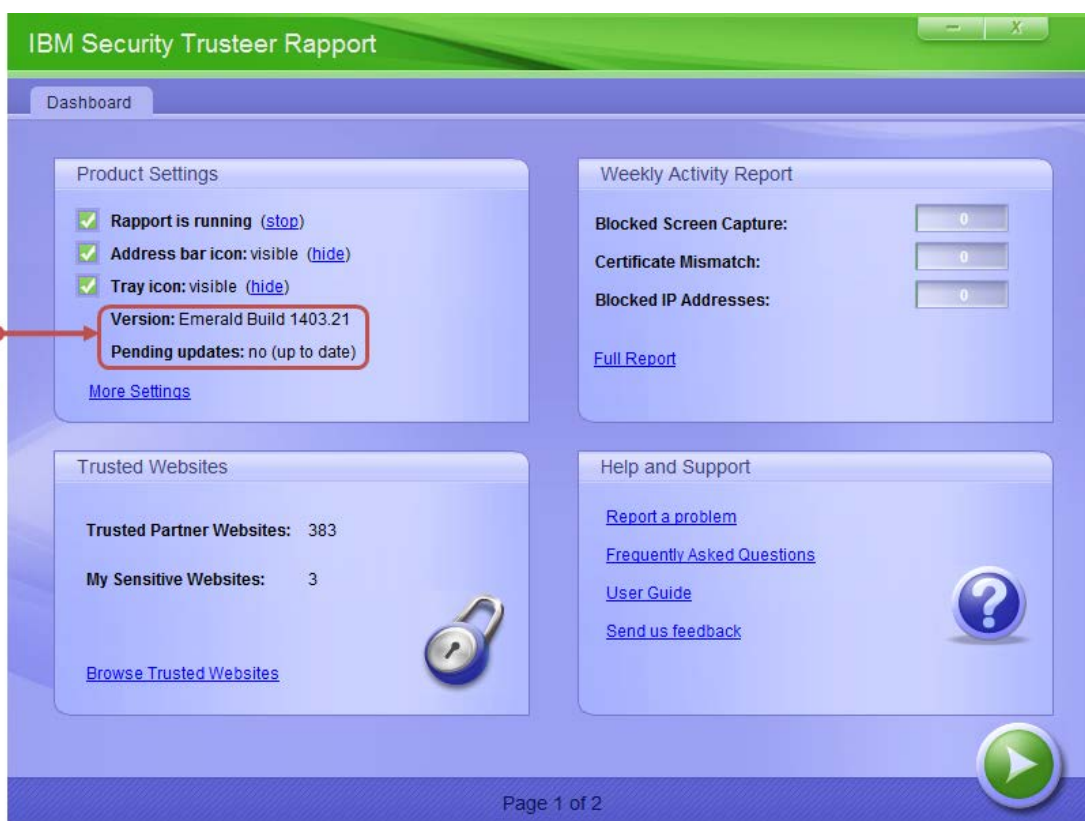
Wyłączanie automatycznych aktualizacji

Domyślnie aktualizacje programu Rapport są wykonywane automatycznie. Aktualizacje pojawiają się niezależnie i bez wiedzy użytkownika. Regularne aktualizacje mają kluczowe znaczenie dla skuteczności działania programu Rapport. Aktualizacje automatyczne można wyłączyć, lecz w takim przypadku program Rapport nie będzie aktualizowany.

➔ Aby wyłączyć automatyczne aktualizacje:

1. [Otwórz Konsole Rapport](#). Obszar Ustawienia produktu zostanie wyświetlony w górnym lewym rogu panelu kontrolnego.

Informacje o wersji i aktualizacjach



2. Kliknij opcję **Więcej ustawień**. Zostanie wyświetlona karta Ustawienia produktu.

3. Usuń zaznaczenie pola wyboru **Automatyczne aktualizacje oprogramowania**. Zostanie wyświetlona karta Weryfikacja użytkownika. Na ekranie wyświetlany jest obrazek zawierający kilka znaków do przepisania. Ma to na celu zabezpieczenie przed uzyskaniem dostępu do Konsoli i wyłączeniem programu Rapport przez szkodliwe oprogramowanie.
4. Wprowadź znaki widoczne na obrazku.
5. Kliknij przycisk **OK**. Automatyczne aktualizacje są teraz wyłączone. Podczas, gdy automatyczne aktualizacje są wyłączone, program Rapport nie jest aktualizowany do czasu jego ręcznej aktualizacji. Więcej informacji można znaleźć w sekcji [Ręczne aktualizowanie programu Rapport](#).

11. Deinstalowanie programu Rapport

Zdecydowanie zaleca się zdeinstalowanie programu Rapport. W przypadku trudności z programem Rapport należy przesłać wniosek o wsparcie na stronie <http://www.trusteer.com/support/submit-ticket>. Na czas rozwiązywania problemu można [zatrzymać program Rapport](#) bez deinstalowania go.

Program Rapport oferuje tylko jedną metodę deinstalacji, co pozwala chronić go przed nieuprawnioną deinstalacją.

Uwaga: Jeśli program Rapport zainstalowano z konta administratora systemu Windows, wówczas można zdeinstalować go wyłącznie po zalogowaniu się z konta administratora.

[Deinstalowanie programu Rapport \(Windows 8 i Windows 7\)](#)

[Deinstalowanie programu Rapport \(Windows XP\)](#)

Uwaga: W przypadku napotkania trudności przy deinstalowaniu programu Rapport oraz w celu uzyskania informacji na temat deinstalowania programu Rapport za pomocą narzędzia do bezpiecznej deinstalacji należy zapoznać się z informacjami pod adresem:
<http://www.trusteer.com/support/uninstalling-rapport-using-safeuninstall-utility>.

Co oznacza pole wyboru **Usuń ustawienia wszystkich użytkowników na ekranie podczas deinstalowania?**

Pole wyboru **Usuń ustawienia wszystkich użytkowników** pojawiające się w oknie dialogowym Deinstalowanie programu IBM Security Trusteer Endpoint Protection powoduje usunięcie wszystkich zmian wprowadzonych w programie Rapport, w tym dodanych serwisów oraz haseł, na których ochronę się zdecydowano. Po zaznaczeniu tego pola wyboru, jeśli użytkownik zdecyduje się na ponowne zainstalowanie programu Rapport w przyszłości, program nie zapamięta żadnych z wprowadzonych zmian.

Deinstalowanie programu Rapport (Windows 8 i Windows 7)

→ Aby zdeinstalować program Rapport:

1. Otwórz Panel sterowania.
2. W menu **Programy** kliknij opcję **Deinstalowanie programu**.
3. Kliknij dwukrotnie pozycję Trusteer Endpoint Protection na liście programów. Zostanie wyświetlony komunikat z prośbą o potwierdzenie.
4. Kliknij przycisk **Tak**. Zostanie wyświetlone okno dialogowe programu Rapport przedstawiające najnowsze zdarzenia, których program Rapport pomyślnie zapobiegł.
5. Kliknij przycisk **Kontynuuj**. Zostanie wyświetlone kolejne okno dialogowe, oferujące pomoc w zakresie problemów technicznych z programem Rapport. Aby kontynuować deinstalowanie, należy zamknąć wszystkie otwarte pliki i aplikacje.
6. Kliknij opcję **Nie; zdeinstaluj teraz**. Program Rapport ukończy proces deinstalowania. Po zakończeniu procesu deinstalowania zostanie otwarte nowe okno przeglądarki z prośbą o opinię o programie Rapport oraz kilkoma prostymi pytaniami.

Deinstalowanie programu Rapport (Windows XP)

→ Aby zdeinstalować program Rapport:

1. Otwórz Panel sterowania.
2. Kliknij opcję **Dodaj/usuń programy**.
3. Odszukaj na liście programów pozycję Trusteer Endpoint Protection i kliknij przycisk **Zdeinstaluj/Zmień** obok programu Trusteer Endpoint Protection. Zostanie wyświetlony komunikat z prośbą o potwierdzenie.

4. Kliknij przycisk **Tak**. Zostanie wyświetlone okno dialogowe programu Rapport przedstawiające najnowsze zdarzenia, których program Rapport pomyślnie zapobiegł.
5. Kliknij przycisk **Kontynuuj**. Zostanie wyświetlone kolejne okno dialogowe, oferujące pomoc w zakresie problemów technicznych z programem Rapport. Aby kontynuować deinstalowanie, należy zamknąć wszystkie otwarte pliki i aplikacje.
6. Kliknij opcję **Nie; zdeinstaluj teraz**. Program Rapport ukończy proces deinstalowania. Po zakończeniu procesu deinstalowania zostanie otwarte nowe okno przeglądarki z prośbą o opinię o programie Rapport oraz kilkoma prostymi pytaniami.

12. Aktualizowanie programu Rapport

Aby przeprowadzić aktualizację programu Rapport do nowej wersji, należy zainstalować nową wersję bez uprzedniego deinstalowania poprzedniej. Proces instalowania jest taki sam, jak w przypadku standardowej instalacji, obejmuje jednak kilka dodatkowych kroków.

Instrukcje instalacji można znaleźć w sekcji [Instalowanie programu Rapport](#). W trakcie procesu instalowania wyświetlany jest następujący ekran:



Ten ekran pojawia się podczas instalowania nowej wersji bez deinstalowania istniejącej. Po wyświetleniu tego ekranu wybierz opcję **Tak - chcę tylko przeprowadzić aktualizację**. Kliknij przycisk **Dalej** i kontynuuj proces instalowania jak zwykle.

Uwaga: Jeśli program Rapport został już zainstalowany z konta administratora systemu Windows, wówczas można zainstalować program Rapport bez deinstalowania bieżącej wersji wyłącznie po zalogowaniu się z konta administratora.

W trakcie procesu instalowania zostanie wyświetlony komunikat zabezpieczający z prośbą o potwierdzenie:

Ten ekran zostanie wyświetlony, ponieważ kreator instalacji wymaga zamknięcia istniejącej wersji programu Rapport w celu zainstalowania nowej wersji. Z uwagi na zabezpieczenie przed możliwością wyłączenia programu Rapport przez szkodliwe oprogramowanie każde jego zamknięcie wymaga potwierdzenia przez użytkownika. Po wyświetleniu tego ekranu należy wprowadzić znaki widoczne na obrazku i kliknąć przycisk **Zamknij**. Proces instalacji jest kontynuowany jak zwykle.

Po zakończeniu procesu instalowania w oknie komunikatu może zostać wyświetlony następujący tekst:

Nastąpiła aktualizacja programu Trusteer Endpoint Protection do nowszej wersji. Niektóre nowe funkcje programu Trusteer Endpoint Protection będą dostępne dopiero po ponownym uruchomieniu.

Mimo wyświetlenia tego komunikatu komputer jest chroniony. Zaleca się jednak ponowne uruchomienie komputera tak szybko, jak to tylko możliwe.