*Com os cumprimentos da Kaspersky Lab*

# Segurança Móvel e BYOD

PARA

# LEIGOS®

*Trazido para você por*

KASPERSKY lab

**Georgina Gilmore**
**Peter Beardmore**

# *Sobre a Kaspersky Lab*

A Kaspersky Lab é a maior fornecedora privada do mundo de soluções de proteção de endpoints. A empresa é classificada entre as quarto maiores fornecedoras do mundo de soluções de segurança para usuários finais.* Ao longo de mais de 15 anos de história, a Kaspersky Lab permaneceu inovadora em segurança de TI, e oferece soluções de segurança digital efetivas para grandes empresas, pequenos e médios negócios, e consumidores. A Kaspersky Lab atualmente opera em quase 200 países e territórios em todo o mundo, oferecendo proteção para mais de 300 milhões de usuários em todo o mundo.

Descubra mais no site http://brazil.kaspersky.com/produtos-para-empresas/.

* A empresa foi classificada como quarta no International Data Corporation's Worldwide Endpoint Security Revenue por fornecedor em 2011. A classificação foi publicada no relatório IDC 'Worldwide Endpoint Security 2012–2016 Forecast and 2011 Vendor Shares' (IDC #235930, Julho de 2012). O relatório classificou fornecedores de software de acordo com as receitas de vendas de soluções de segurança de ponto em 2011.

# Segurança Móvel e BYOD

PARA

LEIGOS®

Uma marca Wiley

## Edição Limitada Kaspersky

# Segurança Móvel e BYOD

PARA LEIGOS®

Uma marca Wiley

## Edição Limitada Kaspersky

Por Georgina Gilmore
e Peter Beardmore

PARA LEIGOS®

Uma marca Wiley

**Segurança móvel e BYOD Para Leigos,® Kaspersky Lab Limited Edition**

Publicado por
**John Wiley & Sons, Ltd**
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
Inglaterra

Para detalhes sobre como criar um livro personalizado Para Leigos para o seu negócio ou organização, entre em contato com CorporateDevelopment@wiley.com. Para informações sobre licenciamento da marca Para Leigos para produtos ou serviços, entre em contato com BrandedRights&Licenses@Wiley.com.

Visite a nossa página em www.customdummies.com



Wiley também publica seus livros em uma variedade de formatos eletrônicos. Algum conteúdo que aparece impresso pode não estar disponível em livros eletrônicos.

ISBN: 978-1-118-66252-6 (livro eletrônico)

# Conteúdo num piscar de olhos

# Introdução

Bem-vindo ao guia *Segurança móvel e BYOD Para Leigos* – seu guia para alguns dos pontos principais a considerar quando estiver habilitando o acesso móvel aos seus sistemas de negócio ou ampliando a sua política móvel existente. Com as dicas e indicações contidas neste livro, almejamos ajudá-lo a evitar comprometer a sua segurança e incorrer em quaisquer penalidades regulatórias ou jurídicas.

Assim como com qualquer alteração no processo de negócio, é sábio considerar mais do que apenas os benefícios. Potenciais desafios podem surgir quando dispositivos móveis são usados para acessar dados e sistemas corporativos. Além disso, se você decidir adotar o BYOD (Traga o Seu Próprio Dispositivo), você tem benefícios adicionais porém, também problemas adicionais com os quais lidar. Então vale a pena estar bem preparado . . . e é por isto que escrevemos este livro.

## Sobre este livro

Este livro pode ser pequeno, mas está cheio de informações sobre os benefícios e desafios que o acesso móvel e BYOD podem trazer.

Para iniciativas de acesso móvel, não há uma abordagem para 'todos os tamanhos'. O livro oferece dicas e indicações valiosas para ajudar os negócios a considerar seus próprios requisitos exclusivos – antes de formularem sua própria estratégia. *Segurança móvel e BYOD Para Leigos* pode ajudá-lo a cuidar de:

- Benefícios e desafios gerais do negócio.
- Considerações jurídicas e responsabilidades potenciais.
- Implicações de RH – contratos, políticas e treinamento.
- Desafios de segurança de TI e soluções.

## Suposições falsas

Para ajudar a garantir que este livro ofereça as informações que você precisa, fizemos algumas suposições:

- O negócio que você gerencia ou possui ou para o qual trabalha está interessado em oferecer – ou ampliar – acesso aos seus dados e sistemas de negócio, através de dispositivos móveis.
- Você está procurando por algumas dicas sobre estratégia móvel ou BYOD.
- Você precisa de algumas indicações sobre potenciais problemas jurídicos – e como evitá-los.
- Você pretende garantir que os dados confidenciais permaneçam confidenciais.
- Você está procurando informações sobre tecnologias que possam ajudar a evitar que o acesso móvel torne-se uma fonte de ataques ao ambiente corporativo.

## Como este livro é organizado

*Segurança móvel e BYOD Para Leigos* está dividido em seis capítulos concisos e repletos de informações:

- **Capítulo 1: Por que dispositivos móveis e BYOD?** Explicamos os benefícios e desafios que você enfrenta.

* **Capítulo 2: Explorando as coisas assustadoras:** malware, perda e outros riscos. Este capítulo lhe informa dos principais riscos de segurança, agora e no futuro.
* **Capítulo 3: Conhecendo os aspectos legais.** Fique do lado certo da lei com as informações aqui.
* **Capítulo 4: Refinando a sua estratégia, política e diretrizes BYOD.** Decida quem envolver e como implementar a sua iniciativa móvel.
* **Capítulo 5: Selecionando o software de segurança: os recursos 'obrigatórios'.** Saiba que tecnologias ajudam a proteger os seus dados e sistemas.
* **Capítulo 6: Dez perguntas para ajudá-lo a refinar a sua estratégia.** Use estas perguntas como uma lista de verificação útil.

## Ícones usados neste livro

Para que você possa encontrar as informações que deseja ainda mais facilmente, estes ícones destacam o texto principal:


O alvo chama a sua atenção para conselhos principais.


O ícone da palavra amarrada destaca informações importantes para ter em mente.


Preste atenção nestas armadilhas potenciais!

4

# Aonde ir a partir daqui

Você pode investigar este livro da forma que quiser, ou lê-lo de capa a capa. É uma leitura rápida e fácil! Qualquer forma que escolher, garantimos que vai considerá-lo repleto de conselhos úteis sobre como garantir que o seu acesso móvel ou projeto BYOD tenha sucesso.

# Capítulo 1

# Por que dispositivos móveis e BYOD?

*Neste capítulo*

- Avaliando os benefícios
- Considerando os desafios a tratar
- Decidindo se BYOD é o certo para o seu negócio
- Acompanhando . . . quando a decisão já está tomada

Neste capítulo, daremos uma olhada em alguns dos benefícios e desafios que os negócios enfrentam ao considerar a introdução de acesso móvel a dados e sistemas corporativos. Também consideramos as implicações de iniciativas "Traga Seu Próprio Dispositivo" (BYOD, na sigla em inglês).

## O que significa acesso móvel?

No ambiente de negócio acelerado de hoje, as empresas que oferecem aos seus funcionários um acesso rápido e conveniente para a maioria dos seus dados e sistemas corporativos – através de dispositivos móveis – podem ganhar uma vantagem significativa sobre seus concorrentes. Dar aos trabalhadores remotos ou móveis

acesso aos dados mais atuais e oferecer aos funcionários a capacidade de carregar informações em sistemas corporativos, tem o potencial de melhorar a eficiência e a agilidade do negócio.

Contudo, mesmo com benefícios significativos a oferecer, há alguns problemas a tratar se a iniciativa de acesso móvel do seu negócio não afetará a segurança dos seus dados e sistemas corporativos, ou resultar em falha do negócio em seguir a legislação e os requisitos de conformidade. Ninguém quer ver o negócio sendo processado pelos clientes e parceiros de negócio – ou o diretor executivo sendo pessoalmente responsabilizado por alguma penalidade legal . . . especialmente quando você é o diretor executivo!


Apenas para novatos, aqui estão alguns dos desafios que os negócios enfrentam ao considerar a introdução de acesso através de dispositivos móveis:

- Quais são as implicações se os sistemas corporativos forem acessados de fora do firewall corporativo?
- Algum dado corporativo deve ser armazenado em dispositivos móveis?
- Há risco de que o negócio possa perder controle sobre onde os dados estão exatamente?
- Há penalidades legais potenciais para a empresa e seus diretores?
- O que você pode fazer para evitar que malware e crimes cibernéticos obtenham acesso aos seus sistemas corporativos?
- Como você pode motivar a sua força de trabalho para tomar precauções sensíveis para evitar problemas jurídicos e de segurança?

- Você pode garantir a segurança contínua dos dados corporativos se um dispositivo for perdido ou roubado?
- Há problemas de conformidade associados ao acesso móvel de seus dados e sistemas corporativos?

# Por que se preocupar com BYOD?

Com o recente interesse crescente em *iniciativas BYOD* – através das quais os funcionários recebem permissão para usar seus próprios dispositivos móveis para comunicações de negócio – há muito foco nos benefícios adicionais que BYOD pode oferecer, tanto para empregadores quanto para funcionários. Se houver benefícios potenciais a serem ganhos, precisamos verificar mais de perto.

## Conhecendo os benefícios

Para os empregadores, BYOD oferece benefícios potenciais:

- **Custos reduzidos:** O negócio não tem que comprar e atualizar dispositivos móveis. O ciclo de atualização para dispositivos móveis pode ser muito curto – especialmente se alguns dos seus funcionários 'simplesmente tiverem de ter' o último e melhor dispositivo, assim que for disponibilizado. BYOD pode descomplicar com sucesso o negócio dessa burocracia.
- **Melhor produtividade:** Com muitos usuários experimentando algo que está cada vez mais perto de um 'relacionamento pessoal' com seus dispositivos móveis, não é surpreendente que os funcionários geralmente apreciem poder escolher sua própria marca e modelo. Se o funcionário já estiver

familiarizado com um dispositivo em particular, isto pode ajudar a eficiência quando estiverem usando-o para tarefas relacionadas ao trabalho.

Para os funcionários, BYOD também pode oferecer vantagens:

- **Melhor proteção:** Com empregadores responsáveis tomando atitudes para salvaguardar seus sistemas e dados, os funcionários podem encontrar-se em uma melhor situação beneficiando-se de software de segurança móvel que ajuda a proteger seus próprios dados pessoais no dispositivo, com custo assumido pelo seu empregador.
- **Facilidade de uso:** Os funcionários podem escolher o dispositivo que gostam de usar – e isto, por sua vez, pode ajudar a melhorar a produtividade ainda mais para o empregador!


Quando um novo funcionário é contratado, há muito a aprender. Se ele conseguir usar seu próprio dispositivo para executar tarefas de trabalho – em vez de ter de aprender a operar um dispositivo móvel diferente – ele pode começar mais rápido.

## Ok . . . qual é o segredo?

Antes de ser bem convencido sobre os benefícios potenciais e começar a considerar BYOD como prática padrão, vamos fazer uma pausa. Sim, há benefícios. Também é verdade que, à medida que os funcionários vão de uma empresa para a outra, o 'hábito BYOD' provavelmente se espalhará. Então este enorme BYOD parece estar ganhando força e os negócios sentem a pressão de crescimento atropelar seu próprio programa BYOD.

Contudo, isto não significa obrigatoriamente que BYOD é a coisa certa para o *seu* negócio. Pode ser, se você elaborar uma estratégia que garanta que você possa capitalizar os benefícios potenciais – sem cair em nenhuma das armadilhas. Por outro lado, alguns negócios podem se sair bem afastando-se do BYOD – talvez por que do setor da indústria no qual operam, do tipo de dados que processam, dos códigos regulatórios que se aplicam a eles . . . ou de todos esses fatores.


BYOD traz os seguintes desafios:

- O negócio tem pouco ou nenhum controle sobre a gama de tipos de dispositivos e Sistemas Operacionais (OS) sendo utilizados, então a tarefa de gerenciar todos estes diferentes dispositivos poderia levar a uma sobrecarga de gerenciamento.
- Há um risco maior de segurança comprometida no dispositivo (desde dados, anexos ou aplicativos infectados), que pode levar a infecções ou ataques no resto da rede corporativa.

Se o negócio suportar o uso de absolutamente qualquer dispositivo móvel que o usuário escolher, isto poderia absorver muitos recursos. Comparado com uma política de dispositivos de propriedade corporativa – onde uma pequena seleção de dispositivos e sistemas operacionais são avaliados e usados – BYOD traz uma gama de dispositivos e OS que precisam ser habilitados e protegidos. Algumas tecnologias inteligentes podem ajudar você a lidar com isto, mas esteja ciente no que você está se metendo.

BYOD pode significar que o negócio tem de dar suporte ao uso de iOS, Android, BlackBerry, Symbian, Windows

Mobile e Windows Phone – incluindo diferentes versões de cada um desses OS. Além disso, há um potencial para novos OSs no futuro, e eles também terão de ser suportados.

## Você diria Não ao Diretor Executivo?

BYOD se estabeleceu de forma que nenhuma outra tecnologia fez previamente. Quando uma empresa atualiza os laptops, computadores de mesa ou servidores, o departamento de TI obviamente tem um papel decisivo no projeto – vetar fornecedores potenciais, avaliar o desempenho de tecnologias concorrentes, definir contratos de suporte e manutenção e gerenciar mudanças. Mesmo que adotar uma nova estratégia de acesso móvel tenha muitos requisitos técnicos, de suporte e segurança, o ímpeto inicial por trás da introdução de novas tecnologias móveis normalmente tem sido muito menos formal.

Considere a situação onde o diretor executivo obtem o último 'dispositivo da moda'. Este é um dispositivo tão legal que é criogênico! Agora, não seria ótimo usar este dispositivo para acessar sistemas de negócio? 'Isto poderia revolucionar a forma como fazemos negócio', dizem – e em pouco tempo, o projeto de acesso móvel está em execução.

## Rendendo-se ao inevitável

Agora, tem alguém – e queremos dizer alguém que valorize sua carreira – que vá dizer, 'Nada disso, José'? Mesmo se o seu diretor executivo se chamar José, isto pode acabar com a carreira de alguém (e se ele se chamar Frank, ele

pode pensar que você tem trabalhado demais). Mesmo um simples 'Opa . . . espera aí, tem coisas importantes que temos de considerar aqui' poderia ser benéfico. Mas quem negará os desejos do diretor executivo? Afinal de contas, ele tem um motivo válido: este dispositivo poderia fazer muito para revolucionar os processos de negócio principais e potencializar a eficiência.

## Colocando tudo de volta no trilho

Então, no nosso cenário, a empresa e a equipe de TI tem que encontrar uma forma de fazer isso acontecer. Mas isto pode deixar a equipe de TI e o cara da segurança confusos. O cavalo está pronto – agora temos de construir um estábulo. O próximo capítulo ajuda-o a considerar o que está em risco . . . e como você pode colocar tudo de volta no trilho.

# Capítulo 2

# Explorando as coisas assustadoras: malware, perda e outros riscos

*Neste capítulo*

- Descobrindo a escala dos riscos de segurança
- Entendendo a natureza de ameaças diferentes
- Mantendo a segurança ao usar Wi-Fi
- Uma olhada no que nos aguarda no futuro

Poucos negócios imaginariam executar sua infraestrutura de TI sem as tecnologias adequadas de segurança em vigor. Contudo, em geral, os negócios e seus funcionários são muito menos conscientes dos riscos de segurança e dos problemas associados ao uso corporativo de dispositivos móveis. Afinal de contas, é apenas um telefone ou um tablet – e todo mundo já perdeu um ou dois deles em algum momento . . . certo?

Bem, pode ser assim, mas os smartphones e dispositivos de hoje estão a milhares de quilômetros de distância daqueles antigos telefones que pareciam tijolos que precisavam de duas pessoas para carregá-los. Se alguém

perdesse um telefone em um taxi em 2003, teria perdido muitos detalhes de contato e seria muito inconveniente... mas isto seria tudo que estaria perdido. Não seria como se a segurança do seu empregador tivesse sido comprometida de alguma forma!

Mas nos dias de hoje, é uma história muito diferente.

## É um computador no seu bolso?

Seu dispositivo móvel é realmente um poderoso computador que é capaz de armazenar uma enorme quantidade de dados. Se você usá-lo para suas tarefas de trabalho, alguns dos dados no seu telefone ou tablet poderiam comprometer seriamente a segurança da sua empresa se estas informações caíssem em mãos erradas. Com todas as suas senhas armazenadas no seu dispositivo, os criminosos poderiam obter acesso direto às suas informações pessoais e acesso direto aos sistemas corporativos da empresa.

Os principais riscos à segurança incluem:

- Perda de dados – como resultado de um dispositivo sendo perdido ou roubado.
- Roubo de identidade – se um criminoso roubar seu dispositivo e entrar nas suas contas online.
- Malware que rouba informações.
- Vazamento de informações, através de conexões Wi-Fi maliciosas.

### Onde eu coloquei o meu telefone?

Dispositivos móveis modernos são tão pequenos e finos que está mais fácil do que nunca perder um deles. Para alguns usuários, isto é quase inevitável. Então todos os usuários devem tomar algumas precauções simples. É aconselhável confiar apenas em um simples PIN quando uma frase de senha poderia ser mais segura?

Precauções e tecnologias podem ajudar no evento de um dispositivo ser perdido ou roubado. É possível armazenar dados de uma forma que seja totalmente ilegível se o seu telefone for roubado. Além disto, tecnologias especiais de segurança móvel podem lhe dar acesso remoto ao seu telefone perdido, então você pode executar uma série de recursos de proteção e antirroubo no dispositivo. Há mais sobre isto adiante neste livro (mas se você quiser avançar para ver como é feito, veja o Capítulo 5).

## Loucura de malware móvel

O recente crescimento no uso de smartphones resultou em um crescimento correspondente nas atividades dos bandidos que procuram oportunidades de prejudicar vítimas inocentes. Como todos estamos usando nossos telefones para fazer mais coisas – como comprar, transações bancárias e tarefas do trabalho – criminosos cibernéticos estão atacando os smartphones.


Criminosos cibernéticos! Eles podem parecer seres empolgantes de filmes de ficção científica, mas na realidade são equipes profissionais bem financiadas que estão constantemente desenvolvendo formas cada vez mais sofisticadas

de roubar o seu dinheiro e a sua identidade . . .
e lançar ataques contra negócios.

Apesar de o primeiro malware móvel ter sido descoberto em 2004, o crescimento nos ataques de malware era relativamente baixo até 2010. Mas então . . . KABOOM! Em 2011, o volume de novos malwares que estava almejando dispositivos móveis excedeu todo o volume dos 6 anos anteriores. E 2012 presenciou outro crescimento sêxtuplo em malware móvel. Agora está óbvio que os dispositivos móveis tornaram-se um alvo principal para criminosos e malware.

## Não baixe a sua guarda

Por que o rápido crescimento em malware móvel? Isto se deve em parte ao crescimento no número de smartphones que estão em uso, parcialmente por causa das coisas para as quais usamos os nossos smartphones e parcialmente por que alguns de nós somos culpados por baixarmos a nossa guarda. Este último ponto é algo que podemos ajudar a resolver.

Dispositivos que são utilizados para transações bancárias online, compras e para acessar os sistemas do empregador, chamam a atenção dos bandidos. Assim os riscos estão crescendo. Contudo, muitos negócios que não levariam os riscos de segurança para dentro da sua rede de TI estão inocentemente deixando estes dispositivos ganharem acesso a dados preciosos . . . sem pensar suficientemente sobre o que acontece com as informações que acessam e as senhas que usam.

## Algum dispositivo móvel é seguro?

Criminosos estão atualmente almejando algumas plataformas móveis muito mais que outras. Apesar de definitivamente haver riscos que afetam dispositivos Apple

e BlackBerry, o maior aumento recente nas ameaças tem sido naqueles ataques que almejam dispositivos Android. Então, os usuários Apple e BlackBerry precisam se preocupar?

De forma simples – sim!

Considere o mundo de laptops e computadores de mesa. Muitas pessoas e negócios se sentiam mais seguros usando Macs em vez de PCs. Contudo, esta condescendência passada sobre a possibilidade de ataques contra Macs claramente foi um grave erro. Houve muitas instâncias bem documentadas de ataques de malware que atacavam especificamente Macs – e o número de ataques está crescendo.

De forma similar, para dispositivos móveis pode ser um erro confiar em uma plataforma particular como mais segura que outra, e continuar confiando nisso e não fazer nada sobre a segurança. Assim que criminosos cibernéticos percebem uma oportunidade – e percebem que a guarda está baixa para uma plataforma específica, como resultado de algum senso errado de segurança – este é o momento no qual os bandidos mais provavelmente escolhem um novo alvo.

Isto aconteceu no passado. Antes do recente aumento de ameaças Android, o foco principal de ataque era a versão móvel do Java. Antes disso, os alvoseram dispositivos baseados em Symbian e Windows CE. Assim, esta é uma situação acelerada e constante – e os negócios precisam tentar se antecipar aos bandidos.

E também, lembre-se que o risco não é apenas do malware. Os dados que estão em qualquer dispositivo perdido ou roubado são vulneráveis se o dispositivo não estiver protegido. Além disto, um criminoso pode roubar dados em qualquer dispositivo se um usuário conectar-se a uma rede Wi-Fi não confiável.


Quando o usuário desbloqueia ou vincula o seu dispositivo móvel – para desbloquear o dispositivo para uso na rede de outro provedor ou para remover as limitações no intervalo das aplicações que podem ser executadas – é um pouco como remover a porta da frente de uma casa. Desbloquear ou vincular um dispositivo compromete a segurança. Neste ponto, não interessa que OS ( Sistema Operacional ) o dispositivo está usando. O risco é real. Você deseja desbloquear dispositivos que acessam a rede corporativa?

# Malware móvel principal

Atualmente, três tipos principais de malware existem:

- Cavalos de Troia
- Programas de Adware
- Botnets e outras ameaças de hacker

## Cavalos de Troia SMS

Apesar do nome, não há nada clássico ou mitológico sobre este tipo de malware. Eles são uma forma particularmente dissimulada de tirar dinheiro da pessoa ou negócio que paga a conta de telefone. Após um dispositivo ter sido infectado por um Cavalo de Troia SMS, o criminoso gera receitas fazendo o dispositivo automaticamente – e silenciosamente – enviar várias mensagens de texto para números de telefone de classificação principal. Ok, então não é necessário invadir um banco, ou o seu negócio se é a empresa que paga a conta. Mas ainda vale a pena proteger seus dispositivos contra estes ataques, especialmente porque podem potencialmente prejudicar a reputação do negócio.

## Outros Cavalos de Troia

Os dois outros tipos comuns de Cavalos de Troia são backdoors e programas espiões – e ambos são projetados para extrair dados dos dispositivos móveis. Backdoors fornecem ao atacante controle remoto sobre o dispositivo – permitindo que o atacante faça praticamente qualquer coisa com ele. Programas espiões 'vazam' dados do telefone para o atacante – por exemplo, mensagens pessoais ou o número serial do dispositivo.

## Aquele anúncio que o enlouquece

Programas de Adware parecem bem inofensivos, mas o problema com eles é que não apenas exibem anúncios . . . eles também carregam funções adicionais e não autorizadas. Por exemplo, eles podem fazer coisas como mudar a página inicial do navegador do usuário sem a permissão do usuário.

## Botnets

Deixamos o pior por último. Este grupo de ameaças amplia o conceito de backdoor para permitir controle remoto de dispositivos móveis em massa – às vezes dezenas de milhares de uma vez.


Botnets são redes de dispositivos comprometidos com a segurança que são explorados por hackers para funcionar como parte de uma rede que espalha malware e ataques. Esta é uma rede com a qual você não quer que seu dispositivo se junte.


Às vezes, ameaças móveis são ataques híbridos que combinam a funcionalidade de uma backdoor, um Cavalo de Troia SMS e um bot.

Como ataques voltados a empresas frequentemente começam com hackers reunindo informações que podem ajudar o criminoso a personalizar e configurar seu ataque contra uma empresa específica, ataques de hacker e botnet são uma fonte de grande preocupação. Há muitas instâncias bem documentadas destes tipos de ataques sendo lançados através de computadores de mesa e servidores. Agora, com muitos negócios falhando em garantir segurança adequada nos dispositivos móveis dos seus funcionários, os criminosos estão vendo os dispositivos móveis como um meio fácil – e cada vez mais produtivo – de reunir informações e obter acesso à rede corporativa.

## Wi-Fi, Wi-Fi, Por Que, Wi-Fi?

Quando os funcionários acessam redes públicas Wi-Fi – em aeroportos e hotéis, por exemplo – há um risco de que dados e senhas possam ser *roubados* (ou seja, capturados ilicitamente por criminosos que estejam conectados à mesma rede Wi-Fi). O usuário pode estar apenas fazendo login no Twitter ou Facebook – mas se as senhas forem capturadas, há muitas informações que poderiam beneficiar o criminoso.

Mais e mais grupos criminosos ficam felizes em 'jogar o jogo' e explorar cuidadosamente as informações pessoais que capturaram. Frequentemente a captura de dados pessoais é apenas um meio para um fim. Com estas informações, o criminoso pode assumir a identidade digital do funcionário e depois se comunicar com os colegas do funcionário que não suspeitam de nada. Quando estes colegas recebem comunicações que parecem como se fossem da vítima, quais são as chances de manter a guarda e não revelarem senhas do sistema corporativo ou outras

informações valiosas? Estes ataques de phishing de alvos específicos são conhecidos como *spear phishing*.

## Esta pessoa é quem diz que é?

Ataques de spear phishing podem ser altamente sofisticados. Há muitas informações que as pessoas publicam deliberadamente em sites de redes sociais – incluindo detalhes de viagens de negócios, férias e família. Então o atacante pode colocar muito conhecimento pessoal na sua comunicação com os colegas da vítima. Uma mensagem que começa perguntando como foi a viagem de negócios para Viena na semana passada – e depois pede para clicar em um link e inserir seu login da rede corporativa – pode ser bem convincente. Ainda assim, tudo isto resultou de um funcionário acessando um ponto Wi-Fi público legítimo (e, portanto, inseguro).

E criminosos não apenas capturam informações que são enviadas usando uma rede Wi-Fi legítima. Eles também criam pontos Wi-Fi falsos. Estes podem ser configurados virtualmente em qualquer lugar. Criminosos até mesmo se posicionam em estacionamentos da empresa alvo, configuram um ponto de rede – de dentro do seu próprio carro – e depois começam a capturar senhas de funcionários desavisados que usam o ponto falso.


Surfar na Internet usando uma conexão Wi-Fi pública pode ser legal, mas é melhor evitar entrar em serviços específicos que precisam da sua entrada de senhas confidenciais ou outros dados sensíveis.


Muitas pessoas usam a mesma senha em várias contas. Se um criminoso conseguir obter a senha do usuário para uma rede social, isto pode ser tudo que ele precisa para obter acesso à rede

corporativa (e qualquer outra conta online pertencente à vítima). Bingo . . . o criminoso nem precisa usar um ataque de spear phishing.

# Olhando para o futuro: será que poderia ser pior?

Muitas ameaças à segurança existem aqui e agora – o que pode nos aguardar no futuro? É uma aposta segura de que a natureza, sofisticação e alcance das ameaças que exploram dispositivos móveis provavelmente vão aumentar o perigo ainda mais. À medida que o uso de smartphones e tablets continua a aumentar . . . assim também aumentará o interesse de criminosos cibernéticos em explorar qualquer vulnerabilidade nas defesas. Se os negócios rotineiramente falham em devotar esforço suficiente para proteger o acesso móvel, os criminosos continuarão considerando os dispositivos móveis como um caminho de menor resistência aos ataques.

## Perigos drive-by

Para laptops e computadores de mesa, houve um aumento acentuado no número de ataques que exploram vulnerabilidades expostas que estão presentes dentro de aplicações normalmente usadas. Normalmente estão na forma de *ataques drive-by*. Neste tipo de ataque, o usuário inadvertidamente visita uma página que está comprometida e contém um script malicioso. Quando o usuário visualiza a página, o script é executado automaticamente e usa uma vulnerabilidade

exposta – dentro de uma aplicação no computador do usuário – para se instalar no computador. Estes ataques são rotina em computadores de mesa e laptops. Até agora, não vimos nenhum destes ataques baseados em navegador e drive-by almejando dispositivos móveis, mas provavelmente é apenas uma questão de tempo até fazerem isso.

## Outubro Vermelho


O ataque Outubro Vermelho foi um dos primeiros ataques direcionados que não apenas reuniu informações de sistemas de computador, mas também coletou dados especificamente de dispositivos móveis. Dispositivos móveis vão ser alvo de mais ataques direcionados que não apenas acessarão a rede do negócio . . . os atacantes também tomarão atitudes para escalar seus direitos, acessar documentos confidenciais e obter acesso a bancos de dados e informações de contato. Provavelmente os dispositivos móveis se tornarão um aspecto de rotina de ataques de espionagem cibernética nos negócios.

24

# Capítulo 3

# Conhecendo aspectos legais

*Neste capítulo*

- Entendendo suas obrigações de segurança
- Percebendo o que é 'razoável' aos olhos da lei
- Definindo os elementos centrais de uma estratégia móvel
- Pensando sobre problemas de licença

Não importa se a empresa é grande ou pequena, todo negócio armazena dados os quais não pode deixar cair em mãos erradas. Alguns negócios erram em pensar que não vendem para os clientes, que não precisam seguir os regulamentos em relação à segurança de informações identificáveis pessoalmente. Este raramente é o caso. Provavelmente todos os negócios guardam dados pessoais dos seus funcionários. Se a segurança destes dados for comprometida, um processo legal custoso pode acontecer.

Pergunte a si mesmo, o seu negócio armazena qualquer uma das seguintes coisas:

- Listas de clientes e informações de contato?
- Dados de vendas e marketing?
- Propriedade intelectual, conhecimento técnico e designs?

- Detalhes de contas bancárias do negócio?
- Dados sobre funcionários identificáveis pessoalmente?


Se um negócio estiver trabalhando em um projeto conjunto com outra empresa, é provável que cada uma das partes do projeto tenha posse de informações confidenciais que sejam propriedade do outro negócio. Quais seriam as consequências se algum desses dados fosse perdido ou roubado como resultado de negligência? Na melhor hipótese, seria o fim de um lindo relacionamento. Na pior, poderia resultar em um processo legal muito caro, o fim de uma linda parceria e a perda de reputação no setor!

## Então, onde termina tudo isso?

Não é algo que alguém goste de contemplar (exceto talvez alguns jovens advogados ambiciosos), mas é sábio pensar um pouco sobre os riscos jurídicos e o que poderia estar em jogo. Se a sua estratégia móvel der muito errado, há uma chance de que o seguinte poderia estar sujeito a ação legal:

- O próprio negócio.
- Diretores e outro pessoal sênior.

Qualquer pessoa ou entidade que for prejudicada por causa de negligência que leve a uma perda ou vazamento de dados, poderia sofrer um processo legal. Isto poderia incluir clientes, funcionários ou outras empresas que foram parceiras nos seus projetos específicos.


Qualquer parte interessada ou investidor pode ter uma oportunidade de processar – o negócio ou seus diretores – no caso de quebras de segurança.


O custo total da ação legal pode ir muito além da soma de qualquer indenizações, multas e despesas legais. Má publicidade pode prejudicar gravemente a reputação do negócio de uma empresa.

# Regulação e conformidade

Além do risco de ações civis, toda uma gama de regulações e legislação pode se aplicar ao seu negócio. Obviamente, a natureza do escopo de quaisquer regulações varia de território para território e de acordo com o tipo de negócio que você tem. Contudo, pelo menos, provavelmente incluirão um conjunto de regras gerais sobre proteção de dados. Além disto, requisitos específicos e problemas de conformidade se aplicarão se você fizer parte de um setor muito regulado – como serviços financeiros ou tratamento de saúde.

Se a sua empresa opera em vários territórios, é aconselhável buscar aconselhamento sobre os requisitos legais que se aplicam a cada território.


Algumas jurisdições têm regras específicas com relação de dados que cruzam fronteiras. Verifique se está tudo bem deixar um funcionário em um país acessar dados que o negócio armazena em outro país.


Em alguns casos, o pessoal sênior pode ser legalmente responsabilizado pessoalmente – com a possibilidade de multas pesadas ou mesmo sentenças de decretação de prisão.

## Onde está o precedente legal?

Normalmente, quando as empresas tentam colocar suas mãos em requisitos legais associados a introdução de

novas tecnologias no ambiente de trabalho, é importante consultar as leis existentes e os resultados de casos específicos de tribunal interpretando tais leis. Podem ser fontes valiosas de orientação sobre o que é aceitável. Infelizmente, quando se trata de acesso móvel a dados corporativos – ou o uso de BYOD – não há leis específicas e virtualmente nenhum caso relevante de tribunal que os negócios possam consultar.

Se o pior acontecer, e a sua empresa se encontrar em uma posição delicada de ser processada ou acusada judicialmente, qual poderia ser a sua linha de defesa? Na ausência de leis específicas, sua melhor aposta pode ser a capacidade de provar que o negócio tomou medidas razoáveis para evitar a perda de dados ou o vazamento.

## 'Razoável' coloca demandas não razoáveis no negócio?

Então, exatamente como a lei define *razoável*? Esta é uma pergunta capciosa e a resposta varia de acordo com::

- Seu setor da indústria.
- O valor das informações que possui.
- As consequências potenciais da perda de dados.
- O nível de investimento requerido para medidas preventivas.
- O que outros negócios na mesma situação estão fazendo normalmente.

Se o seu negócio possuir vastas quantidades de informações sensíveis – e houver o potencial de causar prejuízo significativo a outras partes se a segurança de qualquer um dos dados for comprometida – este fato influenciará grandemente a visão do tribunal. Nesta

situação, a maioria dos juízes provavelmente teriam dificuldade de decidir se o negócio agiu razoavelmente, caso o negócio tenha economizado alguns milhares de dólares de investimento em algumas medidas de segurança que são comuns dentro do setor específico. Da mesma forma, se esta empresa tiver feito pouco ou nenhum esforço no treinamento da sua equipe sobre as considerações específicas do país, os tribunais podem não ver com bons olhos esta abordagem.

Pergunte a si mesmo, dado o tipo e o valor dos dados que seu negócio mantém – e o custo de medidas preventivas adequadas – o negócio agiu razoavelmente para:

- Proteger seus funcionários?
- Proteger seus clientes?
- Proteger seus parceiros de negócio?
- Estar em conformidade com regulações gerais e específicas?


Uma palavra de precaução: BYOD é um fenômeno relativamente novo. Isto significa:

- Há pouco ou nenhum consenso sobre as melhores práticas dentro de qualquer setor. Então não se surpreenda se os tribunais forem exigentes sobre o que seria uma 'prática de segurança normal' dentro do seu setor.
- Práticas de segurança e expectativas normais de precauções de segurança razoável estão mudando rapidamente. *Razoável* é um alvo em movimento – então certifique-se de que o seu negócio mantém a natureza do razoável em evolução em vista.

# Tomando os primeiros passos em direção de ser razoável

Verificaremos os detalhes dos dispositivos móveis e da estratégia BYOD um pouco mais adiante no livro (ou você pode dar uma olhada agora, no Capítulo 4). Por enquanto, há alguns passos de estratégia básicos que ajudam-no a ficar a frente da lei, os quais destacaremos nas próximas seções.

## Primeiros passos

Primeiro, você precisará de uma política de segurança. Se você for um dos dirigentes dos negócios que já geraram uma política de segurança detalhada e por escrito e a comunicou aos seus funcionários, você precisa fazer duas coisas:

- Ser aplaudido – pois muitas empresas, de todas as formas e tamanhos, ainda têm de fazer o que você já fez.
- Concentre esforços para pensar sobre como você precisa adaptar a sua política de segurança para cobrir os dispositivos móveis e BYOD.

Por outro lado, se o seu negócio ainda tiver que definir uma política de segurança detalhada, agora é o momento ideal para começar.

## Tudo está lá – se você puder encontrar

Modelar e refinar o acabamento da sua política de segurança paga dividendos à longo prazo. Apesar de ser discutível se a política perfeita pode ser elaborada, não deixe que isto seja uma desculpa para não tentar o seu melhor. Uma falta de política perfeita não é necessariamente a área na qual a maioria das empresas falham.

Algumas empresas trabalham bastante, concebem uma política de segurança detalhada e depois a escrevem numa linguagem que um advogado renomado teria dificuldade de decifrar. Se um manual do usuário tiver 1.000 páginas, um texto impenetrável que é cheio de jargão e linguagem floreada – mas os detalhes específicos da política de segurança BYOD estão escondidos nas páginas 836 a 849 – todos podemos imaginar a interpretação do tribunal sobre se a empresa agiu razoavelmente.

Então, planeje escrever a sua política em termos que sejam de fácil entendimento para todos os funcionários. Depois comunique claramente a política de forma que garanta que os funcionários a entendam.


A segurança é como o dever de casa: só faz sentido se você repeti-lo em intervalos regulares. Você precisa atualizar a sua política de segurança para refletir as alterações na forma como você faz negócio ou quaisquer alterações na natureza do risco do seu negócio.

## Treinando e conscientizando

O valor do treinamento nunca deve ser subestimado. Os negócios que recuam à ideia de gastar dinheiro em treinamento devem parar e considerar os custos potenciais que podem resultar de uma falha em oferecer treinamento adequado. Ok . . . agora aqueles custos de treinamento não parecem tão onerosos!

Mais uma vez, a quantidade de treinamento que você precisa para funcionar depende parcialmente do valor e da natureza dos dados que estão em risco – então você precisa oferecer um nível de treinamento que passe no teste do *razoável* jurídico, dada a natureza dos dados e do setor da indústria no qual o negócio opera.


Simplesmente desenvolver uma política de segurança e depois não colocar esforço suficiente para comunicá-la aos seus funcionários – e conscientizá-los sobre os problemas – provavelmente não passa no teste do *razoável*.

O treinamento não precisa ser proibitivamente custoso. Em alguns casos, é apropriado ter cursos de treinamento formais e também testar o conhecimento dos funcionários no final do curso. Contudo, para outros negócios, apenas oferecer um curso seminário web de treinamento talvez seja suficiente.


Qualquer que seja o método de treinamento que você usar, pense sobre com que frequência você deve lembrar os funcionários sobre a política. Um simples e-mail enviado mensalmente ou a cada trimestre pode ser uma forma ideal de reforçar pontos específicos. Se você puder fazer um e-mail chamar a atenção, bem humorado e memorável, isto pode ajudar a passar os pontos principais aos funcionários.

## Conheça 'o implementador'!

Pense em como você vai implementar a sua política de segurança. A implementação pode soar um pouco ditatorial, mas é apenas uma questão de abordagem. Ninguém está defendendo bater nos funcionários que falharem – não interessa que isto seja tentador quando eles perderem metas de vendas ou se atrasarem no relatório mensal! Uma coisa é certa, você não quer desencorajar ninguém a compartilhar detalhes sobre erros inocentes que possam ter cometido ou problemas de segurança que encontraram.

O aspecto mais importante é tomar as ações necessárias para garantir que as violações de segurança simplesmente não aconteçam em primeiro lugar (isto nos leva de volta a garantir que a política de segurança seja razoavelmente concisa e fácil de entender – além disso, todos os funcionários se beneficiam de níveis adequados de treinamento). Então, como a maioria das coisas da vida, quando se trata de aplicar políticas de segurança, a prevenção é bem melhor que a cura.

## Qual a pior coisa que poderia acontecer?

A boa notícia é que na vasta maioria dos casos, quando um funcionário viola parte da sua política de segurança, provavelmente é por causa de ignorância, e não intencional. Espere um minuto! Isto significa que o poder de evitar a violação da política, na verdade, está nas mãos do negócio. Será que estamos ouvindo 'Houve treinamento adequado e uma política escrita de forma clara'?

Circunstâncias extremas acontecem. Então o elemento final em um processo de implementação vê o negócio definindo as penalidades que podem ser aplicadas quando um funcionário deliberada ou repetidamente viola a política de segurança. É o caso de oferecer níveis escalonados de avisos para cada transgressão – talvez culminando na retirada do acesso ao dispositivo móvel/ BYOD? Se o acesso tiver sido retirado, o funcionário ainda conseguirá executar suas tarefas de trabalho? Senão, o procedimento da empresa estabelece o que deveria acontecer depois? Todas estas considerações devem ser claramente definidas e comunicadas, ou não poderão ser legalmente forçadas.


## Você pagou por isto?

Aqui está um problema jurídico que muitas empresas não acham importante: licenças de software e os efeitos do acesso BYOD. O negócio pode ter diligentemente garantido que tem licenças suficientes para cada item de software dentro da sua rede. Contudo, estas licenças permitem que as aplicações sejam acessadas remotamente através de dispositivos BYOD? Algumas licenças permitem este acesso, outras não. Evite fazer suposições perigosas. Verifique os detalhes ou o negócio poderia enfrentar algumas penalidades pesadas.

Saindo um pouco do mundo dos dispositivos móveis, também vale a pena considerar o caso onde um funcionário usa seu próprio laptop para completar tarefas de trabalho quando está em casa. Se estiverem usando sua própria versão 'Estudante e Casa' do software do aplicativo necessário, esta licença provavelmente exclui o uso comercial. Se o negócio estiver encorajando os funcionários a trabalharem em casa – mas não estiver oferecendo as ferramentas licenciadas adequadamente para fazer o trabalho – a empresa pode estar sujeita a penalidades.

# Capítulo 4

# Refinando a sua estratégia, política e diretrizes BYOD

*Neste capítulo*

- Decidindo entre acesso móvel, BYOD e CYOD
- Envolvendo as partes interessadas relevantes
- Gerenciando as expectativas dos funcionários
- Oferecendo aconselhamento contínuo aos usuários

No Capítulo 3, demos uma olhada em alguns dos primeiros elementos para uma estratégia de acesso móvel, e como se relacionam às considerações jurídicas. Neste capítulo, mostraremos os detalhes. Mas primeiro, uma pausa . . .

Mesmo que o interesse em BYOD possa parecer completamente dominante, cada negócio realmente precisa considerar se BYOD é a coisa certa a se fazer – dependendo de cada situação específica.

## Começando com um piloto

Correr rapidamente em direção das inúmeras tecnologias, frequentemente pode ser uma fonte de arrependimento. Mesmo que você decida que BYOD é absolutamente a coisa certa para o seu negócio, vale a pena fazer as coisas passo a passo. Enquanto muitos adotaram precocemente o BYOD em um 'big bang' de projetos em todo o seu negócio, outras empresas já estão aprendendo com estes erros. Esquemas piloto controlados estão se tornando a ordem do dia, pois dão ao negócio uma oportunidade de resolver quaisquer problemas, enquanto que o grupo de usuários BYOD é relativamente pequeno.


Se você escolher executar um esquema piloto ou programa de teste, é uma boa ideia certificar-se de que isto seja executado em um período de tempo adequado. Depois permita um período para definir atualizações adicionais na sua política de segurança e medidas de proteção, após o esquema piloto ter sido completado e antes do uso completo começar.

## O ABC do BYOD e CYOD

Alguns negócios estão recuando um pouco do BYOD e considerando CYOD (Choose Your Own Device – Escolha o Seu Próprio Dispositivo). Em um esquema CYOD, o funcionário não tem uma escolha totalmente livre sobre o dispositivo que vai utilizar. Em vez disso, o negócio emite uma lista de dispositivos aprovados, e se o funcionário quiser obter acesso aos sistemas e dados corporativos, ele tem de usar um dos dispositivos listados.

Muitos dos benefícios do BYOD simplesmente não se aplicam ao CYOD. Se um negócio implementar o CYOD, é

provável que um alto percentual dos funcionários escolha operar um dispositivo diferente para uso pessoal – e se este dispositivo ainda for trazido ao ambiente de trabalho, isto pode causar problemas de segurança, mesmo que não receba acesso a dados corporativos. Apenas o seu negócio pode decidir se CYOD é uma opção viável que atenderá aos seus objetivos.


Para empresas que estão operando uma iniciativa CYOD, ainda é essencial que políticas e verificações estejam em vigor que lidem com a presença de dispositivos pessoais dentro do ambiente de trabalho. Sem dúvida, é fácil evitar que funcionários usem seus dispositivos pessoais para obter acesso à rede corporativa, mas ainda há problemas a serem tratados. Por exemplo, os funcionários receberão acesso ao Wi-Fi corporativo usando seus dispositivos móveis pessoais? Se acesso Wi-Fi for permitido, o negócio deve implementar controles automáticos que evitam visitas às redes sociais durante as horas de trabalho?

## Quem está envolvido na sua implementação móvel ou BYOD?

A resposta curta é . . . todos. Bem, talvez não todos, mas provavelmente pelo menos um representante de cada grupo interessado significativo dentro do negócio. É tentador fazer com que o departamento jurídico dê uma olhada nos aspectos jurídicos e estabeleça as políticas, e depois abra caminho para o pessoal de TI. Grande erro!

Cada grupo interessado tende a olhar para os problemas a partir de uma perspectiva diferente. Isto é algo bom.

Agregar a visão de todas essas perspectivas provavelmente lhe dá uma estratégia de trabalho melhor que tenha uma visão tridimensional de todos os problemas.

- Diretores de vendas, diretores de marketing e diretores de serviço de campo podem todos ter um papel valioso – definindo quais aplicações corporativas e dados sobre seus trabalhadores remotos precisam ser acessados quando estiverem no campo.
- A equipe jurídica fornecerá o conhecimento técnico para ajudar a garantir que nenhum problema jurídico ou de conformidade exista.
- A equipe de Recursos Humanos (RH) pode ajudar com todos os aspectos de relações dos funcionários – desde ajudar a desenvolver novas políticas até treinamento e emenda dos contratos de emprego. (Consulte a próxima seção para obter mais informações sobre o papel da equipe de RH na implementação.)
- A equipe de IT aconselhará sobre tecnologias – incluindo segurança. Seu conhecimento e suas habilidades serão fundamentais durante a implementação, e serão uma equipe que tem que lidar com qualquer tecnologia ou problemas de segurança de dados que resultem da ampla gama de tipos de dispositivos móveis que os funcionários podem usar para acessar os sistemas corporativos.

## Leve-me ao seu líder

A equipe de RH provavelmente está bem posicionada para ter um papel de liderança para refinar os elementos principais da sua estratégia móvel e BYOD. Afinal de contas, eles têm uma ampla experiência em desenvolver políticas, documentá-las – de forma amigável aos

funcionários – planejando cursos de treinamento e motivando os funcionários para que sigam as melhores práticas.

O pessoal de RH também tem a atitude mais esclarecida para definir os objetivos que estão por trás das políticas e diretrizes que você precisa – e os objetivos por trás do treinamento necessário. Eles podem tomar conta do que é necessário para emendar contratos de trabalho e definir regras disciplinares diante de quebras de segurança. Para esta última tarefa, eles são a equipe que não apenas focará na punição dos transgressores. Seu pessoal de RH entende que o objetivo é dar aos seus funcionários todas as ferramentas e informações que precisam para garantir que os problemas não surjam, para que haja menos necessidade de penalidades.

Contudo, o mundo não é perfeito, então você ainda precisará da ajuda deles para definir como os transgressores serão tratados. Novamente, provavelmente a equipe de RH está bem posicionada sobre como definir procedimentos disciplinares justos e imparciais.


Vale a pena perceber que se ocorrerem violações da política, isto poderia ser a oportunidade perfeita para reavaliar as políticas da empresa. Talvez não tenha sido culpa do funcionário – talvez a política seja inadequada ou precise de alguns ajustes.

Como discutimos no Capítulo 3, treinamentos – e possivelmente cursos e lembretes de atualização contínuos – são um elemento vital para garantir que a sua iniciativa BYOD tenha sucesso, seja segura e menos provável de levar a empresa a ter dificuldades jurídicas. Quando se trata de planejar e executar programas de treinamento, quem é melhor qualificado que a sua equipe de RH?

## Deixando claro que o acesso não é garantido

Sempre que um negócio adota um novo método de trabalho, ele precisa tomar cuidado para garantir que quaisquer alterações nos processos de trabalho não possam ser interpretadas como uma mudança fundamental nos termos e condições de trabalho. Obviamente, a equipe de RH é a sua fonte interna de conhecimento técnico para evitar estes problemas e garantir que a introdução de novas tecnologias não crie um senso de direito.

O programa BYOD deve ser considerado como algo que a empresa pode oferecer a funções específicas do trabalho – mas não tem que oferecer o programa a todos que operam dentro dessas funções. Da mesma forma, o negócio precisa expressar as regras em termos que deixem claro que o privilégio de fazer parte do esquema BYOD pode ser retirado, e que a participação na iniciativa BYOD não tem nada a ver com uma mudança fundamental no relacionamento de trabalho.

## Esclarecendo . . . não contradizendo!

Tendo considerado todas as partes interessadas para consulta através das fases iniciais de definição de políticas e estratégia, e depois implementando o seu acesso móvel ou programa BYOD, também vamos dar abertura para qualquer funcionário que tenha perguntas legítimas mesmo depois de ter completado todo o treinamento necessário.

Oferecer um único ponto de contato que seja capaz de oferecer aconselhamento informado é um grande passo. O que você realmente quer evitar é uma situação na qual um funcionário levante uma pergunta com o departamento

de marketing e receba uma resposta . . . levante a mesma pergunta com a TI e receba uma resposta ligeiramente diferente . . . e consulte a equipe de RH e receba uma terceira resposta.

Seu ponto único de contato pode incluir representantes de diferentes grupos de interesse, assim cada um pode focar em questões que lhes sejam específicas. Contudo, ao fornecer um único endereço de e-mail para perguntas – e certificando-se que seus funcionários o conheçam – você oferece um local para todas as perguntas.


Políticas, diretrizes e contratos que não são claramente entendidos – ou são sujeitos a aconselhamento contraditório de diferentes contatos especialistas dentro da empresa – podem ser totalmente não executáveis se problemas jurídicos surgirem.

# Capítulo 5

# Selecionando o software de segurança: os recursos 'obrigatórios'

*Neste capítulo*

- Defendendo-se contra ataques de malware
- Simplificando a segurança móvel, incluindo a Gerenciamento de Dispositivos Móveis (MDM, na sigla em inglês)
- Protegendo os dados em dispositivos perdidos ou roubados
- Facilitando o gerenciamento da segurança – em todos os endpoints

Quando se trata de segurança, o acesso móvel traz uma necessidade de uma nova mentalidade. No passado, era mais fácil de confiar em qualquer dispositivo que estivesse dentro da rede corporativa. Agora, com os dispositivos móveis e BYOD sujeitos a riscos de segurança e ataques que estão presentes no mundo externo, como podemos confiar no comportamento destes dispositivos quando estão operando dentro da rede corporativa?

# Cuidado com as vulnerabilidades!

Enquanto que anteriormente tudo que você tinha de fazer era proteger o seu perímetro com um firewall de primeira linha e depois garantir a posse de provisões de segurança adequadas para cada endpoint dentro deste perímetro, a segurança não é mais tão simples. O acesso móvel muda o jogo completamente – e pode criar algumas vulnerabilidades na segurança.

Na realidade, parte do seu perímetro de segurança ainda está ao redor do seu negócio, mas parte dele também está ao redor de cada usuário. Há um limite invisível ao redor de cada um dos seus usuários móveis, e precisa ser protegido.

## Aqui vem a cavalaria

Adicionar qualquer novo tipo de endpoint à rede corporativa tem o potencial de aumentar a carga ao departamento de TI – especialmente quando se trata de segurança. A mobilidade traz seus próprios desafios exclusivos. No Capítulo 2, damos uma olhada em várias ameaças . . . e há muitas ameaças e riscos de segurança para os desavisados. Combine estas ameaças com a natureza dispersa do perímetro de segurança do negócio e as coisas ficam um pouco assustadoras.

Bem, seria bem assustador se não houvesse nada que pudéssemos fazer para conter estes riscos e defender estes perímetros. Felizmente, os mocinhos – na forma dos fornecedores de software de segurança – tem muitos truques inteligentes para ajudá-lo a defender o seu dispositivo, seus dados e seu ambiente corporativo

Há algumas ótimas tecnologias que ajudam a proteger os seus dados corporativos e a manter o malware fora da sua rede. Enquanto alguns elementos da segurança móvel estão por aí já há algum tempo, novas tecnologias foram reveladas apenas recentemente. Então aqui está uma breve introdução sobre os recursos e capacidades que você deve querer garantir que estejam incluídos em uma solução de segurança móvel cuja qual você escolher para o seu negócio.

## Anti-malware

A rápida ascensão do malware e outras ameaças que estão atacando dispositivos móveis significam que os negócios precisam instalar software anti-malware que seja capaz de proteger os dispositivos móveis contra os mais recentes vírus, spyware, Cavalos de Troia, worms, bots e outros códigos maliciosos. Soluções que apenas usam tecnologias anti-malware tradicionais baseadas em assinatura, não são mais suficientes para garantir a proteção adequada. Então é uma boa ideia procurar uma solução de segurança que inclua análise heurística – assim como proteção baseada em assinatura – para que seja capaz de defender-se contra malware documentado e também aquelas novas ameaças para as quais ainda não existe uma assinatura.

Soluções rigorosas anti-malware também incluem tecnologias anti-spam, para filtrar chamadas indesejadas e textos que tentem alcançar o dispositivo móvel. Então isto significa menos distrações para a sua força de trabalho.

Recursos anti-phishing também são vitais para ajudar a evitar visitas inadvertidas a sites falsos ou fraudulentos que tentam roubar informações.


### Beneficiando de uma solução híbrida

*Soluções híbridas anti-malware* – que combinam tecnologias anti-malware que rodam nos seus dispositivos, além de serviços baseados em nuvem – podem oferecer um nível ainda maior de proteção. Enviando dados atualizados no último minuto aos seus sistemas e dispositivos sobre as últimas ameaças emergentes, serviços de nuvem podem trabalhar com tecnologias anti-malware baseadas em assinatura e heurísticas que estejam rodando no seu dispositivo . . . assim você se beneficia de uma segurança multicamada.


Aqui estão algumas coisas adicionais para observar para a sua solução anti-malware:

- Com que frequência os bancos de dados anti-malware são atualizados? Frequentemente, pequenas atualizações ajudam a garantir que você esteja protegido contra nova ameaças, sem colocar uma carga desnecessária nos seus sistemas.
- A solução permite que você execute verificações sob demanda, assim como verificações agendadas?

## Gerenciamento de Dispositivos Móveis (MDM)

Uma solução MDM integrada pode ajudar a facilitar toda uma nova administração e tarefas de segurança em toda uma gama de diferentes dispositivos e Sistemas Operacionais (OS), incluindo:

- Implementar o agente de segurança em cada dispositivo – com recursos que permitem que você provisione software de segurança Over the Air (OTA) remotamente.
- Simplificar a implementação de políticas de segurança nos dispositivos.
- Separar dados pessoais e corporativos em cada dispositivo – e habilitar a 'exclusão seletiva' de dados corporativos, sem excluir os próprios dados pessoais do usuário.
- Possibilitar o uso de tecnologias de criptografia nos dispositivos.
- Controlar como as aplicações são abertas e usadas.
- Gerenciar acesso à Internet.
- Detectar a presença de dispositivos invasores.
- Proteger os dados quando um dispositivo é perdido ou roubado.

## Conteinerização

Agora, esta é uma forma muito inteligente de resolver os problemas que podem surgir de ter dados tanto pessoais quanto corporativos armazenados em um dispositivo móvel BYOD. Algumas soluções de segurança permitem que o negócio defina contêineres especiais em cada dispositivo – com todos os dados corporativos sendo armazenados no contêiner. Desta forma o administrador pode definir políticas específicas para os dados que são mantidos no contêiner corporativo no telefone. Por exemplo, todos os dados dentro do container podem ser automaticamente criptografados.

Quando um funcionário deixa a empresa – ou se um dispositivo for perdido ou roubado – a conteinerização ajuda a tratar um problema importante. Se os dados corporativos tiverem sido armazenados em um contêiner no dispositivo móvel – de tal forma que estejam totalmente separados dos dados pessoais do usuário – é fácil para o administrador remover (excluir seletivamente) os dados corporativos sem afetar as informações pessoais do usuário.

## Criptografia

Criptografar dados sensíveis é uma ótima forma de garantir que quaisquer informações que estejam armazenadas em um dispositivo móvel possam ser virtualmente inúteis para qualquer ladrão. Muitos dispositivos móveis incluem tecnologias de criptografia de dados – sendo assim é apenas uma questão de garantir que sua solução de segurança móvel escolhida tenha recursos MDM que facilitem que seus administradores gerenciem esses recursos embutidos de criptografia.


Como invadir um telefone pode comprometer seriamente a proteção, algumas soluções de segurança móvel buscam ativamente dispositivos invasores que os funcionários estejam usando. Assim o software de segurança evita que o telefone invasor ganhe acesso aos sistemas e aplicativos corporativos. Também pode haver um recurso que permita que você exclua todos os dados corporativos do dispositivo invasor.

## Controle de aplicativo

Os recursos de controle de aplicativo são uma forma poderosa de controlar a abertura de aplicativos. Seus administradores podem definir uma lista negra

de aplicativos e garantir que nenhum destes aplicativos tenha permissão de rodar no dispositivo móvel do usuário, mas todos os outros aplicativos podem ser abertos.


Usar o controle de aplicativo para definir a política de permissão padrão permite que qualquer aplicativo rode no dispositivo do usuário, a menos que tal aplicativo esteja na lista negra.

Definir uma política de negação padrão impede que todos os aplicativos, rodem com a exceção daqueles aplicativos que estão na lista branca.

## Controle da Internet

O controle da Internet dá ao negócio a capacidade de monitorar e filtrar a atividade de navegação dos usuários – frequentemente o controle pode ser selecionado de acordo com a categoria, conteúdo ou tipo de dados. Os administradores de sistemas da empresa podem permitir, proibir, limitar ou auditar as atividades dos usuários em sites específicos ou categorias de sites.

## Socorro, meu telefone foi roubado!

Todos conhecemos esse sentimento, no fundo do estômago, quando perdemos algo precioso. Bem, apenas imagine como você se sentirá se o seu dispositivo móvel for perdido ou roubado – e estiver cheio de informações corporativas confidenciais. Como isto vai parecer ao chefe?

Não tema. Se o negócio tiver tido a prudência de investir em uma solução de segurança que inclui recursos antirroubo, há muito que pode ser feito para remediar a situação e evitar que dados e sistemas corporativos sejam ilegalmente acessados.

## Bloqueando seu telefone perdido . . . e excluindo os dados dele

Primeiro há capacidades de bloqueio remoto. Desta forma, você pode enviar ao seu telefone uma mensagem de texto especial que bloqueia o uso do dispositivo para que o ladrão não possa acessar os dados ou aplicativos no celular. Algumas soluções de segurança até mesmo deixam que você exiba uma mensagem especial na tela do telefone, para que você possa pedir que o telefone seja devolvido.

Se você estiver convencido de que seu telefone não apenas escorregou pelas almofadas do sofá, algumas soluções de segurança lhe dão acesso remoto a uma função de exclusão dos dados que pode excluir totalmente os conjuntos de dados selecionados no telefone – ou excluir todos os dados e reiniciar o telefone para suas configurações padrões de fábrica. Então você pode ter perdido o telefone, mas ainda conseguirá evitar que os bandidos explorem quaisquer dados que estejam no seu telefone.

## Encontrando o seu telefone

Que tal tentar localizar o seu telefone? Há até mesmo soluções que lhe dão detalhes da localização aproximada do dispositivo – usando GPS ou conexões Wi-Fi para calcular o paradeiro do telefone.

É claro, o ladrão pode ter trocado o cartão SIM rapidamente no seu dispositivo. Novamente, a tecnologia tem a solução: alguns produtos de segurança enviam uma mensagem com o novo número de telefone do dispositivo, para que você ainda possa acessar remotamente quaisquer funções de bloqueio, localização e exclusão de dados.

# Colocando tudo junto

O software de segurança é um elemento essencial para ajudar a manter as informações corporativas seguras e protegidas. Contudo, a segurança da TI – tão vital quanto possa ser – não é realmente uma parte das atividades de negócios centrais da maioria das empresas. Então quanto menos tempo a sua equipe de TI tiver que gastar configurando, implementando e gerenciando a segurança móvel, melhor será para o seu negócio.

Tente descobrir uma solução de segurança que ofereça:

- Todos os recursos de segurança que você precisa – para que você não tenha que integrar ou gerenciar produtos diferentes de fornecedores diferentes.
- Integre fortemente a segurança móvel e MDM abrangente que simplifique as tarefas de gerenciamento – para que você possa devotar mais recursos às suas atividades centrais.
- Altos níveis de integração e interoperabilidade através da segurança para todos os pontos . . . não apenas móveis.
- A capacidade de definir políticas universais em todos os pontos, em vez de ter que definir políticas individuais para pontos individuais.
- Um console de controle único e unificado para todas as tecnologias de proteção.


Para qualquer solução de segurança de TI, a facilidade de uso é vitalmente importante. Se a sua solução de segurança móvel consumir tempo para ser usada, ela será usada ao máximo? Qualquer software que adicione uma camada de complexidade tem o potencial de diminuir a sua segurança, e introduzir novas falhas.

# Capítulo 6

# Dez perguntas para ajudá-lo a refinar a sua estratégia

*Neste capítulo*

- Certificando-se que a sua estratégia cubra todas as bases
- Avaliando os riscos e benefícios
- Verificando se todos estão a bordo

Aqui estão dez perguntas que podem ajudá-lo a refinar sua estratégia móvel e BYOD:

- IO acesso móvel é necessário?
- Quais são os benefícios potenciais do acesso móvel para o seu negócio?
  - Processos melhorados de negócios?
  - Ganhos de produtividade?
- Quais seções da sua força de trabalho precisam de acesso móvel, e quais dados ou sistemas precisam acessar?
- Que sensibilidades há em torno dos sistemas e dados?

- O BYOD poderia oferecer benefícios adicionais para a sua organização?
- Você deve fornecer dispositivos de propriedade da empresa para algumas seções da força de trabalho e permitir uso do BYOD para outro pessoal (dependendo dos tipos de dados/sistemas sendo acessados)?
- Você conduziu uma avaliação de risco completo – incluindo problemas jurídicos – e gerou uma política de segurança?
- Quais são as várias partes interessadas e como cada uma é afetada?
- Que nível de consulta é requerido para cada grupo das partes interessadas?
- O negócio precisará estabelecer novas políticas de RH?
  - Novos contratos para novos funcionários?
  - Anexos para contratos existentes, para funcionários existentes?
  - Programas de conscientização e treinamento?
  - Procedimentos em relação à negligência na segurança dos dados?

Com tanto em risco, se dados corporativos sensíveis caírem em mãos erradas – ou criminosos cibernéticos obtiverem acesso aos seus sistemas corporativos – certifique-se de que a sua estratégia móvel inclua selecionar uma solução de segurança móvel rigorosa. Vire a página para mais detalhes. . . .

# A segurança da qual seu negócio pode depender

Com as tecnologias de segurança premiadas da Kaspersky Lab protegendo os seus sistemas, dados e dispositivos móveis, o mundo do acesso móvel e BYOD não precisa ser assustador.

A segurança da Kaspersky para dispositivos móveis combina tecnologias de proteção poderosas e funcionalidade de gerenciamento de dispositivos móveis (MDM) abrangentes em uma solução fortemente integrada que oferece uma segurança rigorosa e multicamada, bem como um controle de longo alcance e capacidades de gerenciamento. Então é fácil de configurar, implementar e gerenciar segurança móvel de classe mundial.

- Anti-malware
- Anti-spam
- Anti-phishing
- Gerenciamento de Dispositivos Móveis
- Conteinerização
- Gerenciamento de Criptografia
- Controle de Aplicativo
- Controle de Internet
- Recursos antirroubo incluindo:
  - Bloqueio remoto
  - Localização remota
  - Exclusão remota
  - Observação remota de cartão SIM

A segurança da Kaspersky para dispositivos móveis está incluída nas seguintes soluções de segurança integradas para negócios:

KASPERSKY TOTAL SECURITY FOR BUSINESS

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT

Para descobrir como a Kaspersky pode ajudar a proteger cada ponto na sua rede corporativa, acesse http://brazil.kaspersky.com/produtos-para-empresas.

# Dicas essenciais sobre como proteger o acesso móvel e BYOD para o seu negócio

Dar à sua força de trabalho acesso em qualquer momento e em qualquer lugar para sistemas e dados corporativos pode ajudar todos a fazer um trabalho melhor. Mas há riscos de segurança. Implemente uma iniciativa BYOD e poderá haver benefícios adicionais . . . e problemas de segurança adicionais. Este livro de fácil leitura traz dicas sobre estratégia, políticas e considerações jurídicas, além de orientação sobre tecnologias de segurança que podem proteger o seu negócio e sua reputação.

- ***Avalie as suas opções – dispositivos móveis da empresa: BYOD ou CYOD (Escolha Seu Próprio Dispositivo)?***
- ***Personalização adequada – adeque a sua estratégia móvel às suas necessidades de negócio específicas***
- ***Consiga 'adesão' – para que os usuários façam mais para proteger dados de negócio sensíveis***
- ***Mantenha tudo seguro – com uma segurança móvel fácil de gerenciar***

**Abra o livro e descubra:**

- **Os benefícios para negócios que acesso móvel e BYOD podem trazer**
- **Como evitar problemas jurídicos e regulatórios custosos**
- **Diretrizes sobre como oferecer e gerenciar um programa BYOD seguro**
- **Como selecionar tecnologias que protegem os seus sistemas e dados de negócios**

**Georgina Gilmore** tem mais de 20 anos de experiência no setor de TI. Georgina é diretora de marketing global de clientes B2B da Kaspersky Lab. **Peter Beardmore** juntou-se à Kaspersky Lab em 2008 com especialização em marketing de TI e gerenciamento de produtos. Ele é o diretor sênior de marketing de produtos.

WILEY

**ISBN: 9781118662526**
**Não é para revenda**