Se você tem uma empresa, deve prestar atenção à segurança

Por que a segurança é fundamental para a produtividade

Com um mundo cada vez mais interconectado, a rede da sua organização e seus dados sensíveis se tornam mais vulneráveis a acessos ilegais. Vazamentos de dados podem causar danos devastadores. Um ataque bem-sucedido pode ocasionar perdas financeiras, infrações legais ou regulatórias e prejuízo à reputação da sua empresa.

Apesar do crescente número de ciberataques, muitas organizações adotam uma barreira estática e frágil como proteção. Se essa é sua cultura de segurança, você pode estar sujeito a percepções equivocadas e a uma estratégia de segurança defasada, potencialmente danosa para suas operações.

Fique por dentro das melhores soluções e condutas para manter sua tecnologia segura e sua produtividade maximizada.

Ameaças de segurança são reais e constantes

Protegendo a base dos negócios

Transações financeiras, credenciais, documentações e arquivos são apenas alguns dos inúmeros aspectos das atividades corporativas cotidianas que dependem da confidencialidade, integridade e disponibilidade de seus dados e tecnologia. Se você atende clientes, pacientes ou cidadãos comuns, seu trabalho certamente envolve — e muitas vezes exige — a preservação da privacidade de dados pessoais.

O impacto devastador de vazamentos

Quando seus dados e tecnologia são ameaçados ou comprometidos, a produtividade despenca, a confiança dos clientes enfraquece e os gastos aumentam consideravelmente. Em 2018, a média global de gastos com um único vazamento de dados chegou a custar US$ 3,86 milhões. Diante de consequências nesse patamar, talvez sua organização já tenha um protocolo de segurança implementado. No entanto, se essas iniciativas não forem atualizadas e não incluírem diversas barreiras de defesa, elas podem não ser suficientes para mitigar os ataques, principalmente se eles forem intensificados.

Os crimes cibernéticos aumentam em tamanho e poder

Até hoje, somente cinco por cento dos hackers são processados.[3] A baixa repercussão, aliada aos lucros vultosos, incentivam os criminosos a buscarem vulnerabilidades em seu sistema de defesa constantemente. Com o avanço da tecnologia, as ameaças também se tornam mais sofisticadas e difíceis de detectar. Tomemos como exemplo a inteligência artificial. Testes feitos pela ZeroFOX revelaram que os hackers artificiais são consideravelmente melhores em compor e distribuir golpes de phishing do que os hackers humanos. Some-se a isso a febre da Internet das Coisas (IoT), prevista para alcançar 50 bilhões de dispositivos até 2022.[4] Para os hackers, a abundância de dispositivos interconectados é um grande ponto de entrada para a sua rede e as de outras pessoas também.

Deslizes levam a falhas de segurança

Apesar dos ataques cibernéticos estarem no centro da atenção pública, muitas organizações trabalham com um falso senso de segurança, causado por uma percepção equivocada e medidas insuficientes. Este informativo busca revelar esses pontos de vulnerabilidade e oferecer estratégias para fortalecer suas condutas de segurança, sem reduzir sua produtividade.

US$ 3,86 milhões
foi o custo médio global de um vazamento de dados em 2018[1]

88% dos hackers
conseguem invadir um sistema de segurança cibernético em 12 horas[2]

41% das proteções de rede
das empresas de segurança foram burladas[3]

54% das empresas
responderam a ocorrências envolvendo dispositivos de clientes[3]

38% das empresas
relataram ataques envolvendo dispositivos corporativos[3]

As suposições comuns enfraquecem a proteção

Estas opiniões são frequentes no seu ambiente de trabalho?

As atitudes influenciam as medidas de segurança cibernética que você adota e pratica. Alguns membros da equipe acham que o porte da empresa é suficiente para afastar os hackers; outros consideram o uso de firewall uma barreira aceitável. Há ainda quem busque saídas fáceis por achar que a segurança é um transtorno que reduz a produtividade. Seja qual for sua opinião, saiba que os cibercriminosos estão sempre buscando novas maneiras de burlar seus sistemas de segurança. Se seu sistema não é potente, profundo e consistentemente desenvolvido, sua tecnologia e seus dados não estão bem protegidos. É prudente confrontar os equívocos com a realidade e, assim, reforçar quaisquer fragilidades na segurança de sua organização.

Mito: **Minha organização não é grande o suficiente para ser um alvo.**

Realidade: **Pequenos negócios sofrem 58% dos ataques de malware.[6]**

Se sua empresa é de pequeno ou médioporte, fique atento. Cibercriminosos exploram a falta de recursos e podem até usar sua organização para acessar entidades de maior porte com quem você mantém contato.

Mito: **Nós estamos protegidos pela nossa rede.**

Realidade: **Medidas de segurança comuns, como antivírus e firewalls, quase nunca impedem as ações de hackers; já as tecnologias de segurança de ponta demonstraram ser mais eficazes em inibir os ataques.[2]**

Sua casa estaria segura se você trancasse a porta da frente, mas as janelas e o portão ficassem abertos? Um plano de segurança sólido tem diversas barreiras e é ininterrupto.

Mito: **Nós nunca tivemos falhas de segurança, portanto nosso sistema funciona.**

Realidade: **Talvez uma falha de segurança já nosso tenha ocorrido.**

Pesquisas revelam que uma empresa pode levar até 197 dias para detectar uma falha de segurança.[1]

Mito: **Nós já temos um protocolo de segurança.**

Realidade: **Uma solução isolada é insuficiente para coibir as ameaças que vêm surgindo e expandindo.**

Reflita se seu programa cobre todas as tecnologias conectadas à sua rede e aos seus dados, incluindo soluções, sensores, sistemas e dispositivos corporativos.

Muitas vezes, não é dada atenção suficiente a essas barreiras. Avalie, então, a proatividade de sua organização em atualizar e desenvolver seu protocolo de segurança. Ele deve ser implacável como seus inimigos.

Mito: **Segurança é um assunto muito complicado.**

Realidade: **Um sistema de segurança bem elaborado é intuitivo e fácil de implementar.**

Procure dispositivos corporativos e soluções com múltiplas barreiras de defesa, apoiadas por atualizações diligentes baseadas em padrões rigorosos de segurança. Eles oferecem uma muralha virtual, capaz de proteger seus negócios. Os controles centralizados e automatizados oferecidos por esses dispositivos simplificam as tarefas de TI, ao mesmo tempo que sua segurança intrínseca faz seu trabalho em segundo plano para os usuários finais.

Mito: **A segurança prejudica a produtividade.**

Realidade: **Uma falha de segurança pode paralisar por completo o trabalho — ou pior, seus negócios.**

Uma pesquisa feita pelo Instituto Ponemon demonstrou como a produtividade pode ser prejudicada pelas ações de hackers: [7]

30% das empresas entrevistadas tiveram a produtividade do departamento de TI e do usuário final reduzida [7]

25% relataram inatividade do sistema [7]

23% relataram furtos de ativos de informação[7]

Reforce a segurança com bom senso e com as melhores estratégias

O que você pode fazer para proteger ainda mais sua tecnologia e seus dados? Aplique uma série de condutas recomendadas para proteger suas soluções e dispositivos corporativos. Os dispositivos móveis são particularmente suscetíveis quando estão fora do alcance de firewalls, funcionalidades de gestão de ameaças e filtros de conteúdo e spam, entre outras ferramentas de proteção contra ataques cibernéticos. Portanto, é fundamental reduzir a exposição deles por meio das estratégias eficazes que apresentamos abaixo.

Por fim, não ignore a importância de sua equipe. Eles podem ser seu elo mais forte ou o mais fraco, dependendo da disposição em cooperar. Conscientize seus funcionários. Incentive a participação de todos informando sobre a importância da segurança. Reforce o programa oferecendo recompensas para quem usá-lo e aplicando as regras.

1. Implante um plano com bastante antecedência:

A tecnologia moderna traz possibilidades empolgantes, mas também riscos de segurança. Invista tempo na definição de protocolos de segurança antes de implementar suas novas soluções e dispositivos.

2. Proteja os dados:

Use conexões criptografadas e autenticadas sempre que possível, além de criptografar os dados armazenados em seus dispositivos. Embora seja comum usar senhas e criptografia em aparelhos com conexão sem fio, os dispositivos conectados via cabo/Ethernet também podem precisar dessas medidas (dependendo do tipo de informação contida neles). Lembre-se: se está conectado à sua rede, tenha cautela.

3. Controle os serviços:

Muitos dispositivos oferecem vários métodos de comunicação. Por exemplo, os serviços de rede podem incluir FTP, SNMP e SMTP. Embora esses serviços facilitem o uso e gerenciamento do dispositivo, é uma boa ideia desligá-los quando não estiverem em uso.

4. Mude as senhas:

Os parâmetros padrão costumam representar os métodos documentados de acesso a um dispositivo. Ative senhas de interface de usuário. Elas devem ser fortes e únicas; ou seja, fáceis para você lembrar e difíceis para os outros adivinharem. Não permita o compartilhamento de credenciais e peça para os membros da equipe mudarem suas senhas depois de um determinado período. É importante trocar as senhas de acesso, chaves de acesso e credenciais de autenticação periodicamente.

5. Use um sistema de gerenciamento remoto:

Isso permitirá que você atualize as configurações rapidamente. Quanto mais tempo os dispositivos, soluções e sistemas usarem configurações ultrapassadas, mais fácil será invadi-los. Os sistemas de gerenciamento remoto também aumentam consideravelmente a produtividade da equipe de TI, mas os acessos e permissões devem ser controlados com atenção.

6. Não divulgue as atualizações:

Informe os agendamentos e planos de atualização somente para quem realmente precisa deles. Saber quando ocorrerão as atualizações pode incentivar ações indevidas, ainda que não seja intencional.

7. Monitore os aparelhos fora de alcance:

Conte com um método de monitoramento constante dos dispositivos fora de alcance do seu sistema. Quando suspeitar que um dispositivo foi removido, revogue suas credenciais até confirmar sua localização.

8. Escolha dispositivos que possam ser atualizados sistematicamente:

Invista em dispositivos atualizáveis ao longo de suas vidas úteis para garantir uma compatibilidade contínua com os novos padrões. Também é importante que os sistemas de atualização consigam verificar se os arquivos da atualização não foram corrompidos.

9. Faça um acompanhamento da sua tecnologia:

Adote um plano de descarte para seus dispositivos e soluções. Assim, você poderá remover as configurações dos sistemas corporativos, excluir contas e credenciais de usuários e verificar que os sistemas atuais não tenham sido rigidamente codificados para buscar unidades inativas.

10. Pense no modelo “CID”:

Em todos os estágios da vida útil de um dispositivo ou solução, é prudente implementar o modelo de confidencialidade, integridade e disponibilidade (CID).

a. Confidencialidade:
Assegure que somente as pessoas autorizadas tenham acesso às suas informações e tecnologia.

b. Integridade:
Preserve a estabilidade, precisão e credibilidade dos dados ao longo de sua vida útil.

c. Disponibilidade:
Por último, assegure que os dispositivos e dados estejam acessíveis sempre que o usuário precisar deles.

Adotar novas tecnologias não deveria trazer novos riscos

Você investe em tecnologia para elevar a produtividade e aumentar a eficiência. No entanto, verificar a segurança da tecnologia em questão é vital para a integridade da sua organização. Reflita se a solução e o fabricante atraem ou repelem riscos de segurança. Use as perguntas abaixo como uma referência para avaliar a força da tecnologia de sua empresa.

1 O fabricante acata às melhores práticas de segurança reconhecidas internacionalmente?

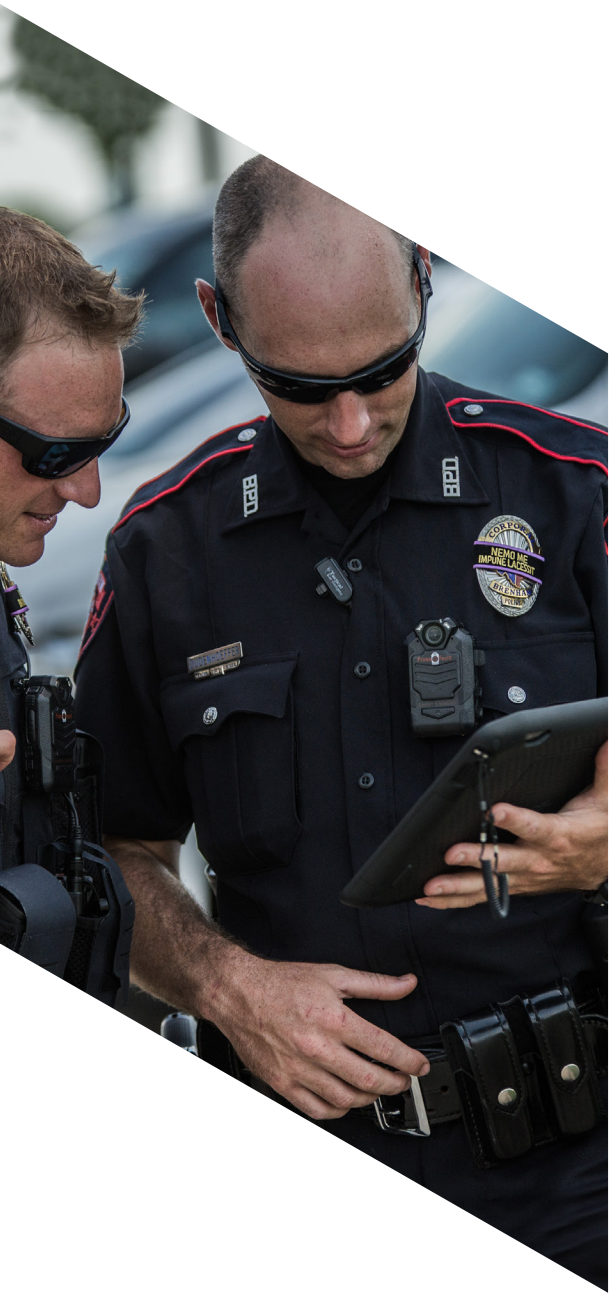
Nem todos acatam. Descubra se os padrões do seu fornecedor de tecnologia são rigorosos. Eles devem proporcionar ferramentas, atualizações e suporte para permitir que sua empresa monitore e responda a ameaças com maior eficácia.

É importante atuar em cada uma dessas etapas de acordo com os padrões internacionalmente reconhecidos de uma organização de segurança, como a Estrutura de Cibersegurança do Instituto Nacional de Padrões e Tecnologia dos EUA:

- **Identificação:** Faça uma avaliação e uma análise de riscos rigorosa para descobrir problemas em potencial
- **Proteção:** Estabeleça garantias, políticas e procedimentos; implemente controles adequados de acesso e auditoria
- **Detecção:** Monitore e inspecione sua tecnologia 24 horas por dia
- **Resposta:** Estabeleça um plano sólido para analisar, selecionar e reagir às ocorrências detectadas
- **Recuperação:** Crie um plano de ação para recuperação; faça melhorias nas correções contínuas de vulnerabilidades e evite ataques futuros

2 A segurança é contemplada da concepção à conclusão?

Uma abordagem de segurança empresarial integrada minimiza riscos por ser projetada para permitir um controle centralizado sobre seus dispositivos e soluções. Descubra se você pode bloquear a tela inicial, os recursos e as interfaces de periféricos, como o USB, Bluetooth®, GPS e comunicação por campo de proximidade (NFC). Busque uma tecnologia que ofereça criptografia de dados granular e com especificações governamentais.



3 Eles verificam a segurança da cadeia de suprimentos?

Sem uma análise minuciosa dos fornecedores, não é possível ter certeza de que a tecnologia foi desenvolvida como deveria. Em um caso, o comprador descobriu um microchip indevido, que poderia ter aberto uma porta de acesso oculta às redes dele. O ideal é investigar as práticas adotadas na cadeia de suprimentos do seu fornecedor de tecnologia.

4 A plataforma de segurança deles é flexível o bastante para atender a suas necessidades operacionais?

Cada empresa é diferente. Isso vale para as tolerâncias de segurança. Você deve estabelecer suas próprias configurações e níveis de segurança de acordo com as necessidades da empresa e de seus departamentos. Lembre-se disso quando for comprar tecnologia. Descubra até que ponto essa solução oferece flexibilidade e controle.

5 Você terá acesso a atualizações contínuas e suporte de segurança durante toda a vida útil da solução?

Sua necessidade de segurança não acaba quando você compra uma tecnologia, portanto o suporte do fornecedor também não deveria. As ameaças são engenhosas. Elas mudam constantemente. Sendo assim, como você pode se antecipar a elas? Escolha um fornecedor que ofereça atualizações de segurança para todo o ciclo de vida da sua tecnologia.

6 Ele será proativo ao avaliar possíveis vulnerabilidades de segurança?

O ideal é que você esteja buscando um parceiro de segurança, e não somente um fornecedor de tecnologia. Um fabricante confiável deve manter sua empresa informada sobre ameaças recentes, recomendar medidas de proteção, examinar suas vulnerabilidades e resolver problemas pertinentes às áreas de necessidade de sua empresa.

7 Ele pode garantir uma resposta ágil e eficaz?

Se uma vulnerabilidade for encontrada, você precisará de suporte imediato e eficiente. Procure uma empresa que tenha procedimentos documentados para relatar e responder às vulnerabilidades. Deve haver recursos adequados disponíveis para a investigação e resolução imediatas de quaisquer vulnerabilidades detectadas no produto.

Zebra – Assegure sua vantagem competitiva

Os produtos, serviços e soluções da Zebra garantem segurança sem comprometer o desempenho. Levamos nosso dever de proteger sua empresa a sério, pois a defesa contra vulnerabilidades de segurança depende de uma abordagem proativa e de múltiplas barreiras de proteção.

Basta olhar para a Zebra para ver nosso comprometimento com a segurança em ação. Ele é evidente nos profissionais de nossas equipes de segurança, design e desenvolvimento, em nossa estrutura de segurança, nas práticas de segurança de nossa cadeia de suprimentos, e na garantia de atualizações preventivas contínuas e alertas ao cliente.

Simples de aplicar e imperceptível para os profissionais na linha de frente. Nossa flexibilidade e recursos podem ser configurados para sua empresa a fim de garantir a segurança e a produtividade. Estamos comprometidos em desenvolver dispositivos, soluções e serviços inteligentes e personalizáveis, que permitam equilibrar os objetivos operacionais e de segurança em tempo real, na vida real.

Conte com a Zebra para fornecer soluções de segurança que não afetarão o desempenho ou a produtividade dos profissionais da linha de frente. Assim, você terá a tranquilidade necessária para implementar seus negócios e estratégias de tecnologia e garantir sua vantagem competitiva.

Fontes:
1. Ponemon, *Cost of a Data Breach Report,* 2018 **2.** Nuix, *Black Report,* 2017 **3.** Carbon Black, *Incident Response Threat Report,* Novembro de 2018 **4.** Juniper Research, 2018 **5.** Ponemon Institute, *Cost of a Data Breach Report,* 2019 **6.** Verizon, *Data Breach Investigations Report,* 2018 **7.** Ponemon, *State of Endpoint Security Risk,* 2018

ZEBRA

Descubra como você pode se sentir e estar mais seguro

Acesse **www.zebra.com/product-security**