Como proteger dados de empresas e dos clientes contra criminosos cibernéticos

Oito estratégias de segurança cibernética para pequenas e médias empresas.

Sobre este Guia eletrônico

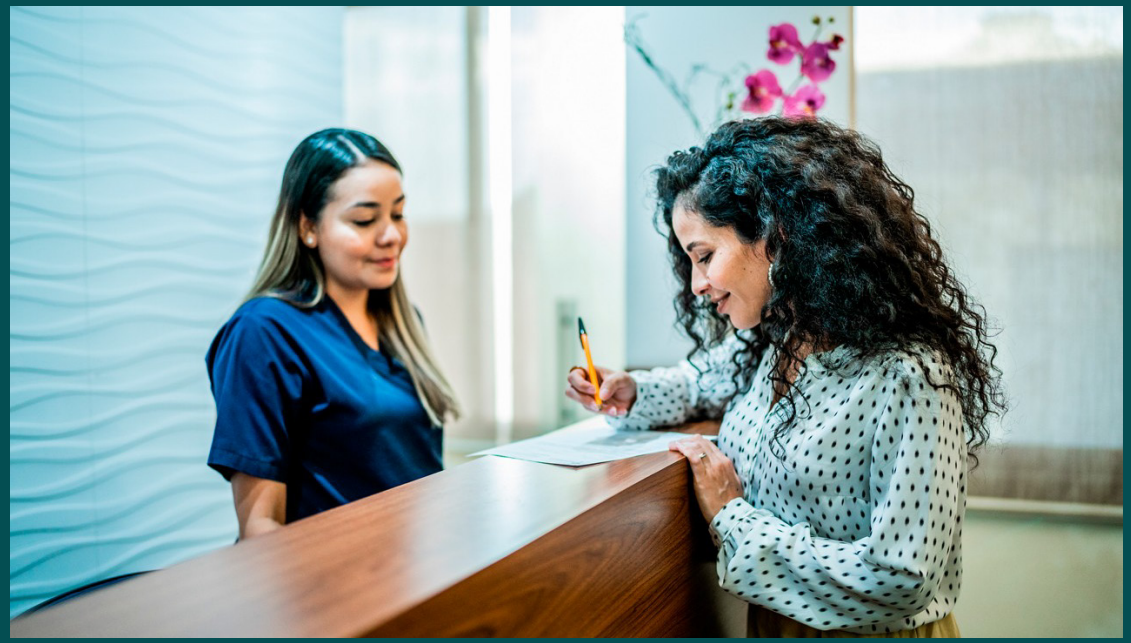
Como um parceiro confiável de TI e segurança para empresas de todos os portes, a Dell Technologies entende os desafios diários de segurança cibernética enfrentados pelas pequenas e médias empresas (PMEs). Neste Guia eletrônico, compartilhamos oito estratégias inteligentes para ajudar a proteger os dados de sua empresa e dos seus clientes contra ameaças cibernéticas.

Sumário

Introdução

Todos nós já vimos as manchetes, os ataques cibernéticos estão acontecendo com mais frequência e atingindo empresas de todos os portes. Para as PMEs, a segurança cibernética não é apenas algo "bom de se ter", é essencial. Os criminosos cibernéticos costumam ter como alvo pequenas e médias empresas, pensando que são mais fáceis de invadir. Embora as empresas geralmente tenham equipes e recursos dedicados de TI e segurança, as PMEs podem não ter. De fato, pesquisas mostram que 35% das pequenas organizações em todo o mundo acreditam que sua resiliência cibernética é inadequada. Esse número aumentou sete vezes desde 2022! Basta um passo errado — um PC sem os patches de segurança mais recentes, informações confidenciais desprotegidas, um clique em um link suspeito em um e-mail de phishing — para expor uma empresa a uma série de problemas, desde contratempos financeiros até dados perdidos e a confiança abalada do cliente.

A boa notícia: Algumas medidas proativas podem fazer toda a diferença. Proteger os dados da sua empresa e de seus clientes ajuda você a se manter confiante, competitivo e pronto para o futuro. ►



Invasores cibernéticos 101

Antes de abordarmos *como* você deve se proteger, é importante entender a mentalidade dos próprios invasores. Os invasores são estratégicos: procuram pontos de entrada fáceis, como PCs sem patches, senhas fracas e redes desprotegidas. Eles frequentemente estudam o comportamento do usuário, identificam identidades e se aproveitam de vulnerabilidades ignoradas. Ao conhecer suas táticas, as PMEs podem priorizar melhor as defesas, identificar atividades suspeitas logo no início e criar uma estratégia de segurança proativa e não reativa. ►

Quem são os invasores?

Os invasores podem variar de criminosos comuns (hackers com má intenção) a Estados-nação. Alguns invasores podem ser facilmente identificados, usando e-mails ou mensagens de texto mal escritos. Alguns podem ter grandes recursos financeiros e lançar ataques muito sofisticados.

Por que eles atacam?

O dinheiro é um motivador fundamental. O crime cibernético global continua crescendo a cada ano, com especialistas prevendo custos anuais chegando a US$ 10,5 trilhões em 2025. Nem é preciso dizer que o potencial pagamento de um ataque bem-sucedido é muito grande para ser ignorado.

Como os invasores atacam?

Os criminosos cibernéticos são implacáveis e estão ficando mais inteligentes com a IA ao seu alcance. Aqui estão alguns métodos que eles usam:

- Ataques a "endpoints", como PCs, são um problema crescente. No estudo Endpoint Security Market Insights da Forrester Research, Inc., realizado em março de 2025, a empresa explica que: "Endpoints estão entre os principais alvos de ataques externos de empresas que enfrentaram uma invasão nos últimos 12 meses".
- Os ataques de identidade também estão aumentando. O phishing continua sendo uma das ameaças mais comuns. É consistentemente um dos principais ataques, frequentemente usado para roubar credenciais e distribuir malware.
- Os ataques à rede, como ransomware, continuam a causar estragos. Pesquisas recentes mostram que as pequenas empresas foram mais afetadas do que as grandes empresas, com 88% de suas violações envolvendo ransomware.

Em resumo, os ataques cibernéticos são altamente lucrativos para os criminosos. O ataque de ransomware bem-sucedido rende, em média, US$ 2 milhões para os criminosos cibernéticos. É por isso que a persistência faz parte da estratégia deles e a proteção deve fazer parte da sua.

Principais riscos de segurança cibernética para PMEs

Comprometimento do dispositivo

Comprometimento da identidade

Comprometimento da rede

1 Saiba o que você precisa proteger

Os invasores buscam dados confidenciais de clientes e funcionários, mas você não pode proteger o que não sabe. Faça o inventário de todos os ativos e dados de TI da sua empresa. Onde os seus dados são armazenados? Quem tem acesso? Quais dispositivos estão na sua rede? Com esses insights em mãos, tome providências. Certifique-se de que os dados sejam armazenados com segurança e restrinja o acesso a informações confidenciais. Conhecer seus dados é um primeiro passo fundamental para protegê-los. ►

2 Trabalhe com fornecedores seguros

Pense na história do cavalo de Troia. Os gregos esconderam soldados dentro de um presente aparentemente inofensivo, que os troianos trouxeram para dentro de sua cidade fortificada. Uma vez que conseguem entrar, os invasores atacam internamente. Os criminosos cibernéticos atuais usam táticas semelhantes: se passam por fornecedores confiáveis, atualizações de software ou hardware. As PMEs frequentemente dependem de muitos fornecedores, o que as torna vulneráveis caso um deles seja comprometido. É por isso que, por exemplo, verificar fornecedores, monitorar a integridade do software e ter visibilidade dos detalhes do envio são essenciais para uma sólida estratégia de segurança cibernética. ►

3 Obtenha PCs com segurança integrada

Todo PC é um possível ponto de entrada para invasores cibernéticos. Os recursos de segurança integrados, como proteções de hardware, inicialização segura e proteções de identidade, ajudam a proteger contra ameaças imediatamente. PCs seguros simplificam o gerenciamento de TI e oferecem defesa mais forte contra malware, phishing e acesso não autorizado. Além disso, lembre-se de que os invasores nem sempre atacam de longe. Um PC autônomo em um espaço público ou compartilhado pode ser acessado fisicamente e comprometido por um colega ou alguém que se passou por equipe ou manutenção. Com recursos limitados e riscos crescentes, tanto físicos quanto digitais, a segurança integrada é essencial hoje em dia. ►

4 Mantenha os PCs atualizados

Os criminosos cibernéticos geralmente exploram falhas conhecidas em sistemas desatualizados, é como esgueirar-se por uma porta destrancada. Ignorar alertas de PC e adiar atualizações pode deixá-lo vulnerável. As atualizações e patches de software são como bloquear essa porta; eles corrigem bugs e falhas de segurança que os invasores podem usar. Patches e atualizações regulares corrigem essas vulnerabilidades, ajudando a proteger os dados da sua empresa e dos seus clientes. Para as PMEs, é uma etapa simples que pode evitar grandes problemas. ►

5 Detecte problemas e corrija-os rapidamente

Só porque você tem PCs seguros e os mantém atualizados diligentemente não significa que um criminoso cibernético não irá atacar. Os invasores podem tentar atacar um único dispositivo dezenas de vezes. Eles podem enviar várias tentativas de phishing por e-mail e por mensagens. Isso aumenta a chance de invasão e acesso a dados confidenciais. É por isso que é importante ter visibilidade em todos os PCs da empresa, na sua rede e em qualquer ambiente de nuvem em que você trabalhe. É aqui que uma camada de software pode ajudar a garantir que você veja tudo e, principalmente, possa agir rapidamente ao detectar atividades suspeitas. ►

6 Use senhas fortes e ative a autenticação baseada em vários fatores (MFA)

Ainda está usando "123456" ou "senha"? Você não está sozinho, mas é arriscado. Credenciais roubadas causam muitas violações. Senhas fortes são essenciais para uma primeira linha de defesa. Dito isso, invasores persistentes encontram maneiras de contorná-las. É por isso que a autenticação baseada em vários fatores (MFA) é importante: ela acrescenta uma segunda camada, reduzindo em 99% a probabilidade de você ser invadido.

Portanto, primeiro, defina senhas fortes.

Em seguida, combine isso com uma segunda maneira de verificar a identidade, como leitores de impressão digital, smart cards ou NFC. Para uma proteção ainda mais forte, armazene as credenciais do usuário em hardware seguro, fora do alcance de malware que tente roubá-las. ►

7 Treine funcionários e teste suas habilidades

Você tem o mesmo nível de segurança de seus elos mais fracos. Infelizmente, o erro humano continua sendo uma das principais causas de violações. Esse erro pode variar desde o adiamento de atualizações críticas do PC até a exposição acidental de dados confidenciais e a reutilização de senhas. Os invasores cibernéticos estão contando com erro humano e comportamento negligente para conseguir entrar por uma brecha na sua empresa. É por isso que o treinamento em segurança cibernética é fundamental. Ele ajuda os funcionários a reconhecer ameaças e a seguir práticas seguras. Ofereça treinamento regularmente e teste suas habilidades. Eles conseguem detectar um phishing? Eles respondem adequadamente? Por quê? Reforce o aprendizado e revele lacunas antes que seja tarde demais. Capacitar os funcionários com conhecimento os transforma em uma forte primeira linha de defesa. ►

8 Tenha um plano de resposta a incidentes

Sempre tenha um plano para o pior cenário. Há muito em jogo. Cada segundo conta quando você sofre uma invasão, e ter um plano de resposta a incidentes em vigor dá à sua equipe um guia claro sobre o que fazer quando algo dá errado. Da detecção da invasão à contenção dos danos e à recuperação com segurança, ter uma estratégia de resposta significa menos tempo de inatividade e um retorno mais rápido aos negócios. Segurança cibernética forte significa ser proativo e estar pronto, independentemente do problema. ►

Principais conclusões

Modernizar o local de trabalho é uma prioridade para muitas organizações que buscam a IA generativa (GenAI) para aumentar a produtividade e aprimorar a experiência dos funcionários. E, embora pesquisas recentes mostrem que 77% das PMEs dizem que a IA/IA generativa é uma parte fundamental de sua estratégia de negócios, a maioria diz que tem medo de que as inovações aumentem sua superfície de ataque. É uma preocupação válida.

À medida que a adoção de AI PCs aumenta e o suporte ao Windows 10 chega ao fim**, esse é o melhor momento para um upgrade.** Desbloqueie os benefícios de desempenho e segurança com os AI PCs mais recentes. ►

Resumo das 8 melhores práticas e como a Dell pode ajudar

1 **Saiba o que você precisa proteger.**
Os serviços Dell podem ajudar a fazer um inventário de seus ativos de TI, redes e dados.

2 **Trabalhe com fornecedores seguros.**
Controles da cadeia de suprimentos da Dell diminuem o risco de adulteração. O design seguro do PC minimiza o risco de vulnerabilidades.

3 **Obtenha PCs com segurança integrada.**
Os PCs Dell vêm com segurança integrada, sem custo adicional.

4 **Mantenha os PCs atualizados.**
A Dell mantém os PCs seguros com patches oportunos. Precisa de ajuda? Experimente uma avaliação de vulnerabilidade com os serviços de segurança da Dell.

5 **Detecte problemas e corrija-os rapidamente.**
Adicione software de parceiros da Dell para monitorar atividades suspeitas em PCs, redes e na nuvem.

6 **Use senhas fortes. Ative o MFA.**
Dê um passo adiante com o Dell SafeID para armazenamento de credenciais baseado em hardware.

7 **Treine funcionários e avalie suas habilidades.**
Conte com os serviços Dell para treinamento em conscientização de segurança dos funcionários.

8 **Tenha um plano de resposta a incidentes.**
Resposta e recuperação de incidentes da Dell pode ajudar.

Tudo pronto para atualizar seus equipamentos? Veja quais PCs são ideais para a sua organização

Encontre AI PCs que atendam às metas de segurança da sua organização. A Dell oferece diversas opções.

Combata ataques a dispositivos, identidades e redes com AI PCs seguros. Mantenha-se protegido e concentre-se no seu dia a dia. ►

Segurança disponível[1]	Dell e Dell Plus	Dell Pro Essential	MAIS SEGURO[2] Dell Pro e Pro Max
Garantia da cadeia de suprimento	•	•	•
Garantia aprimorada da cadeia de suprimentos			•
Disparador de privacidade	•	•	•
Slot de trava de segurança	•	•	•
Leitor de impressões digitais	•	•	•
TPM 2.0	•	•	•
Proteção de credenciais[3]			•
Proteção aprimorada de credenciais[4]			•
Alertas de segurança do PC			•
Atualizações e patches de software	•	•	•
Gerenciamento de PC			•
Chip otimizado para IA	•	•	•
Chip otimizado para segurança			•
Software de antivírus de última geração (NGAV)[5]	•	•	•
NGAV junto com software de detecção de ameaças no PC, rede e nuvem[5]			•
Software de autocorreção, geolocalização e resiliência para PCs			•
Suporte avançado para PCs	•	•	•

--

1 Embora um recurso de PC possa estar disponível em uma linha de produtos, não há garantia que o recurso esteja disponível em todas as plataformas.

2 "Most Secure Commercial AI PCs" (os AI PCs comerciais mais seguros): com base em uma análise interna da Dell de março de 2025. Aplicável a PCs com processadores AMD. Nem todos os recursos estão disponíveis em todos os PCs. Compra adicional necessária para alguns recursos.

3 Autentique via leitor de impressão digital com credenciais armazenadas com segurança no TPM.

4 Autentique via leitor de impressão digital, Smart Card ou NFC com credenciais armazenadas com segurança no ControlVault exclusivo da Dell.

5 Algumas ofertas disponíveis apenas por volume e requerem um número mínimo de licenças. Opções com autorização FedRAMP estão disponíveis.

Dê o próximo passo

Atualize seus PCs.

O suporte ao Windows 10 termina em outubro, deixando muitas PMEs expostas com PCs desatualizados e sem suporte.

Atualize para AI PCs seguros da Dell com processadores AMD Ryzen AI PRO.

Invista em software.

Mantenha os invasores longe com várias camadas de defesa.

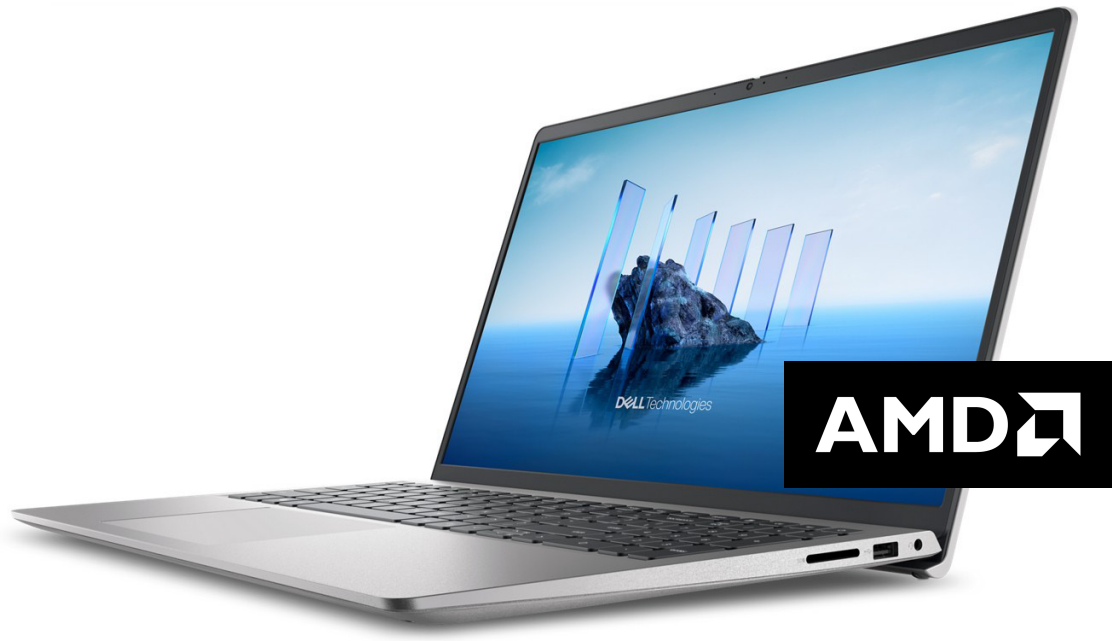
Adicione proteção de software a PCs novos e existentes.

Precisa de ajuda para gerenciar a segurança?

Operações de segurança que você precisa, diretamente de especialistas em segurança cibernética da Dell.

Explore os serviços de segurança gerenciados.

Atualize para os mais recentes AI PCs da Dell com processadores AMD Ryzen AI PRO.



Para saber mais:

Fale conosco: Global.Security.Sales@Dell.com

Acesse: Dell.com/Endpoint-Security

Siga-nos: LinkedIn @DellTechnologies | X @DellTech

Conheça a Dell Technologies

Com recursos limitados, as PMEs precisam ser proativas na proteção das informações da empresa e dos dados dos clientes. Investir em segurança cibernética ajuda a garantir a continuidade dos negócios, protege a reputação e aumenta a confiança do cliente, tornando-se uma parte inteligente e necessária da gestão de uma empresa moderna.

Da mitigação do risco de ataques de ransomware à detecção de atividades suspeitas e resposta a ameaças em tempo real, a Dell está aqui para ajudar você a criar uma estratégia de segurança e implementar soluções de segurança para as necessidades atuais e futuras da sua organização.