Como criar uma estratégia eficaz de cibersegurança?

Guia para pequenas e médias empresas

Digital Security
Progress. Protected.

Nas grandes empresas, geralmente há departamentos inteiros responsáveis por supervisionar a segurança cibernética, construindo estratégias eficazes. Mas no caso das pequenas e médias empresas (PMEs), com apenas alguns especialistas internos em TI, como proceder para garantir que o negócio esteja devidamente protegido, sem haver uma sobrecarga de todas as possíveis medidas?

Aqui estão algumas dicas **de Michal Jankech, vice-presidente do segmento de PME e MSP da ESET.**

Digital Security
Progress. Protected.

Por onde começar?

Na sua maioria, as PMEs dispõem de uma força de trabalho limitada que é encarregada da estratégia de segurança cibernética, nos casos em que há alguma. Por isso, é importante direcionarem o foco às maiores ameaças e investirem sua energia em áreas fundamentais para a continuidade dos negócios.

"As empresas devem adotar uma abordagem baseada em risco, possibilitando identificar as vulnerabilidades mais importantes", explica Jankech, que acrescenta que as PMEs devem abordar, em primeiro lugar, as seguintes áreas:

- **Proteção de dados e criptografia**
- **Proteção de endpoints em multicamadas e restrições de acesso a usuários**
- **Autenticação multifator e atualizações regulares**
- **Provedores de e-mail de alta qualidade e instrução das equipes**
- **EDR ou MDR para uma estratégia madura e abrangente**

Proteção de dados e criptografia

Todos os seus dispositivos estão protegidos com um nome de usuário e uma senha forte? Ótimo. No entanto, há mais ações necessárias para melhorar ainda mais a segurança dos dispositivos. "**Todos os endpoints devem ser criptografados**. Imagine que alguém rouba um dispositivo. A pessoa não consegue ter acesso, pois não sabe o nome de usuário e a senha, porém, é possível acessar os seus dados ao retirar o disco rígido. Certifique-se de que não apenas os dispositivos portáteis, mas também os dispositivos de mesa, sejam devidamente criptografados", sugere Jankech.

"Certa vez, visitei uma instituição de saúde e observei um dispositivo posicionado em um local acessível, sem estar protegido por senha. Assim, alguém poderia facilmente invadir e o roubar, tendo acesso a todos os dados dos pacientes. Cenários como esse podem ser prevenidos com a implementação de medidas eficazes de proteção e criptografia de dados."

Proteção de endpoints em multicamadas e restrições de acesso a usuários

"É fundamental limitar as contas de usuário administrador. Em muitos casos, são as pessoas que podem causar mais danos. No caso de pessoas mal-intencionadas obterem acesso a uma conta de administrador, é possível instalar o que quiserem no dispositivo", explica Jankech.

Além disso, saiba que apenas uma camada de proteção não é suficiente. "É como proteger uma casa de família. Nesse caso, você também usaria medidas que aumentam suas defesas: um portão, portas, um alarme, uma cerca e janelas. Muitas pessoas afirmam que **a era do antivírus terminou**. De fato, a era do antivírus padrão, que funciona apenas por assinatura, acabou. Esse tipo de solução não é capaz de abranger a ampla variedade de ameaças atuais", continua Jankech.

Em vez disso, é recomendado utilizar um **software de segurança de endpoint em multicamadas,** fundamentado nos princípios de machine learning e com proteção baseada em comportamento – incluindo a criação de uma lista de proibições de sites perigosos e o bloqueio de acesso a domínios arriscados, bem como a proteção contra ataques de rede ou vulnerabilidades no protocolo de desktop remoto, que podem ser exploradas de forma indevida.

> **Para pequenas e médias empresas, cabe investir principalmente em prevenção. Reforçar seus sistemas, mantê-los atualizados e utilizar um bom software de proteção de endpoints é fundamental.**
>
> **Michal Jankech**,
> vice-presidente do segmento PME e MSP da ESET

“Não se trata apenas de ter proteção instalada, mas também configurada e atualizada corretamente”, acrescenta Jankech. Por exemplo, garantir que o software de proteção de endpoints não possa ser desinstalado ou ter sua configuração alterada deve ser uma prioridade.

Depois disso, **utilize um console de gerenciamento de endpoints**. “Muitas vezes, existe o pensamento nas empresas de que utilizar um serviço de proteção de endpoints seja suficiente. Porém, não é possível ter a garantia de um funcionamento correto sem o acesso ao gerenciamento por console, que permite supervisionar a rede integralmente. Mesmo em empresas com apenas dez dispositivos, não será possível a verificação adequada, principalmente hoje, momento em que as pessoas trabalham cada vez mais de casa e também viajam”, aponta Jankech. Ao mesmo tempo, o console deve fornecer relatórios que permitam verificar e ter a certeza de que seus sistemas e o tráfego de rede estejam em condições ideais.

Autenticação multifator e atualizações regulares

A autenticação multifator (MFA) deve ser implementada em todos os dispositivos de trabalho, bem como em dispositivos privados. Além disso, deve-se manter todos os sistemas operacionais atualizados com suas versões mais recentes. "A maioria das violações ocorre devido ao roubo de identidade e senhas, ou a uma vulnerabilidade comumente conhecida no sistema operacional, que pode ser utilizada de forma indevida", explica Jankech.

A cada nova versão do sistema operacional, o fornecedor corrige possíveis falhas, diminuindo as chances de cibercriminosos encontrarem uma forma de acessar os dispositivos da empresa. **Atualizações automáticas são recomendadas.** "No caso das PMEs, os ataques de dia zero são incomuns.

Caso esteja utilizando um software feito sob medida, as chances de um ataque direcionado do cibercrime são bastante baixas. Na maioria dos casos, vulnerabilidades amplamente difundidas em softwares comumente utilizados ou de código aberto são o principal acesso do cibercrime à sua empresa", alerta Jankech.

> **"Profissionais da medicina, arquitetura, agências de relações públicas... em todos os casos é necessária uma estratégia de segurança cibernética.**
> **Muitas pessoas não estão cientes, por exemplo, de que alguns documentos são protegidos por direitos autorais e, portanto, devem ter a proteção adequada."**
>
> **Michal Jankech**,
> vice-presidente do segmento de PME e MSP da ESET

Provedores de e-mail de alta qualidade e instrução da equipe

Provedores de e-mail confiáveis também são fundamentais. “Além disso, a equipe de funcionários deve saber detectar um e-mail de phishing. Também é possível informar a cada destinatário que a mensagem chegou de fora da empresa – até mesmo o Office 365 permite marcar e-mails com a tag “externo”, recomenda Jankech.

Periodicamente, é válido investir em treinamento de segurança cibernética para a equipe de funcionários, a fim de aumentar a conscientização. **Leia algumas dicas** sobre como realizar essas formações de forma eficaz e divertida no Guia de Segurança Cibernética da ESET.

Jankech salienta que a maioria das empresas não dispõe dessas medidas básicas implementadas e, algumas vezes, há lacunas ainda maiores na segurança cibernética das grandes empresas. “Algumas empresas ainda hesitam em investir em soluções de segurança cibernética ou acreditam na ideia de que não seriam um alvo, pois sua área de negócio é pouco atraente. Porém, em geral, os ataques cibernéticos não são direcionados. Toda pessoa ou negócio pode se tornar uma vítima”, ressalta o especialista em segurança cibernética.

EDR ou MDR para uma estratégia madura e abrangente

Tendo todos os elementos básicos de segurança cibernética devidamente estabelecidos, é o momento de considerar **ferramentas avançadas de segurança cibernética, como soluções de detecção e resposta de endpoint (EDR).** "É um submercado totalmente novo, construído com base na premissa de que a prevenção sempre terá falhas. Essa parte do conjunto de produtos é aplicável principalmente às grandes empresas, que podem arcar com o luxo de ter diversos departamentos internos de TI e um centro de operações de segurança (SOC) próprio, com operações em tempo integral. Seguir essa abordagem geralmente significa adotar a postura de que, em algum momento, o cibercrime conseguirá atacar o seu sistema com sucesso", acrescenta Jankech.

As soluções EDR identificam anomalias e comportamentos suspeitos na rede, e, idealmente, permitem reações que bloqueiem o processo, ou os sistemas tratam dessas tarefas por meio de regras automatizadas personalizadas. "Embora geralmente utilizadas por empresas maiores, as soluções EDR também podem trazer benefícios para empresas menores.

Elementos essenciais na estratégia de segurança cibernética para as PMEs:

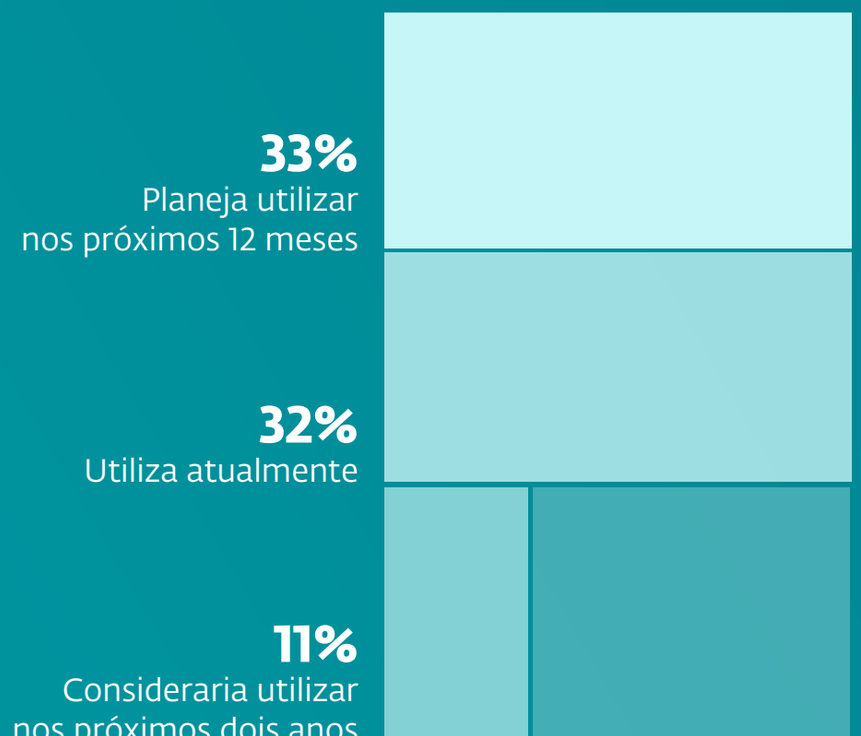
- **Criptografia e proteção de dados**
- **Regras de restrição ao acesso de usuários**
- **Proteção de endpoints em multicamadas**
- **Autenticação multifator e atualizações do sistema operacional**

De qualquer modo, à medida que é necessária uma equipe para gerenciar sua plataforma EDR, recomenda-se que empresas menores com um caso de uso considerem a terceirização desses serviços", acrescenta Jankech.

É aqui que surge a chamada MDR: detecção e resposta gerenciadas. A MDR é uma EDR gerenciada por um terceiro. "A partir de um centro de monitoramento, dezenas ou até centenas de clientes são supervisionados, e costuma haver uma linha direta disponível em tempo integral, à qual é possível recorrer", segundo Jankech.

No entanto, a EDR ou MDR só devem ser consideradas no caso de já haver a cobertura básica. Ao atingir essas condições, o uso de EDR ou MDR aumenta a probabilidade de sua empresa resistir a qualquer ciberataque, mantendo-a segura, mas sempre alerta.

Uso de soluções EDR/ XDR/MDR



Fonte: 2022 ESET SMB Digital Security Sentiment Report.

SOBRE A ESET

Há mais de 30 anos, a ESET® vem desenvolvendo softwares e serviços de segurança cibernética líderes do setor para a proteção de empresas, infraestrutura essencial e consumidores em todo o mundo contra ameaças digitais cada vez mais sofisticadas. De endpoints e segurança móvel à detecção e resposta de endpoints, bem como criptografia e autenticação multifator, as soluções de alto desempenho e fácil uso da ESET protegem e monitoram, discretamente, em tempo integral, com atualização das defesas em tempo real para manter os usuários seguros e os negócios funcionando sem interrupções. As ameaças em evolução requerem uma empresa de segurança cibernética que evolui, permitindo o uso seguro da tecnologia. Contamos com o apoio dos centros de P&D da ESET em todo o mundo, trabalhando a serviço do nosso futuro compartilhado. Para mais informações, acesse www.eset.com/br ou nos siga no LinkedIn, Facebook y Twitter.

Digital Security
Progress. Protected.