ManageEngine
Endpoint Central

BRASILINE

Higiene cibernética essencial **para pequenas e médias empresas**

Índice

O que é higiene cibernética?

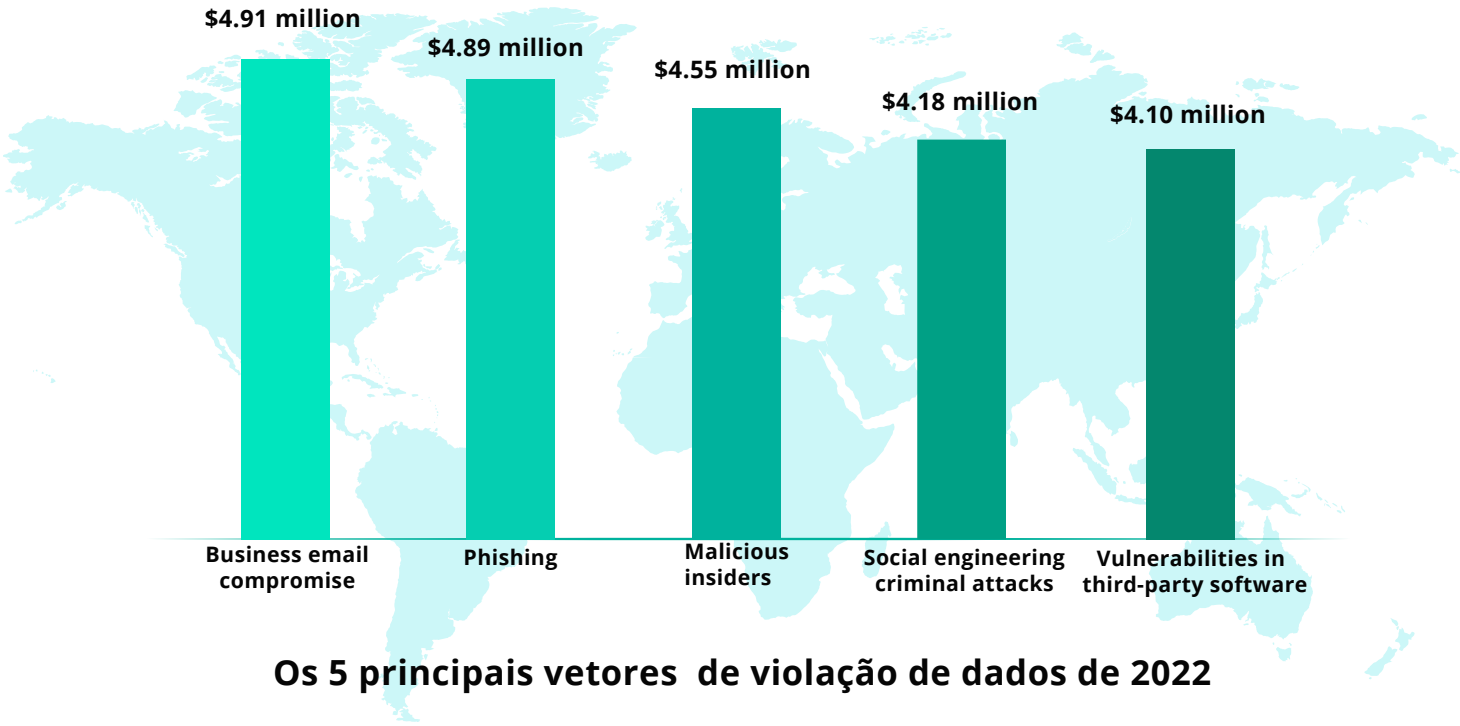
A higiene cibernética é o esforço cuidadoso para se proteger online. É semelhante à higiene pessoal, onde você adota rotinas que o manterão livre de problemas de saúde. Quando se trata de uma organização, a higiene cibernética é um conjunto de procedimentos rotineiros para gerenciar e manter a segurança de indivíduos, dispositivos, dados e redes. São práticas recomendadas essenciais de segurança cibernética que todos os funcionários, não apenas os responsáveis pela segurança, devem seguir. O objetivo final da higiene cibernética é criar um firewall humano que torne impossível para os invasores violar uma rede porque todos na organização estão alertas na frente de segurança.

Por que a higiene cibernética é importante?

No início da pandemia, as empresas recorreram à tecnologia para sobreviver. Mas os cibercriminosos também são rápidos em tirar proveito de uma situação caótica. Em 2022, 79% das organizações concordaram que o trabalho remoto afetou negativamente sua segurança cibernética. Agora que o trabalho remoto veio para ficar, uma boa higiene cibernética pode ajudar você a impedir que os cibercriminosos façam suas coisas ou, pelo menos, torná-lo assim difícil que eles desistam e passem para a próxima vítima.

> ***"Estou convencido de que existem apenas dois tipos de empresas: as que foram hackeadas e as que serão."***
>
> **Robert Meuller, Ex-diretor do FBI**

Até um em cada quatro americanos para de fazer negócios com uma empresa depois que ela sofre uma violação de dados. São erros rotineiros – não acompanhar quais terminais estão se conectando à sua rede, não definir as configurações de segurança adequadas, perder o controle sobre as atualizações de patches , e falha em identificar e corrigir violações - que causam a maioria dos ataques bem-sucedidos.



Os 5 principais vetores de violação de dados de 2022

Além de pesar no bolso, também pode prejudicar a reputação de uma empresa. Perdas financeiras, multas do governo, interrupção de operações, turbulência organizacional, perda de confiança do consumidor e responsabilidade legal são alguns efeitos terríveis de uma violação de dados. Uma boa higiene cibernética não apenas salva sua organização dessas lutas, mas também pode ajudar seus endpoints a funcionar com eficiência máxima, o que significa menos reclamações de sistemas lentos ou tempo de inatividade.

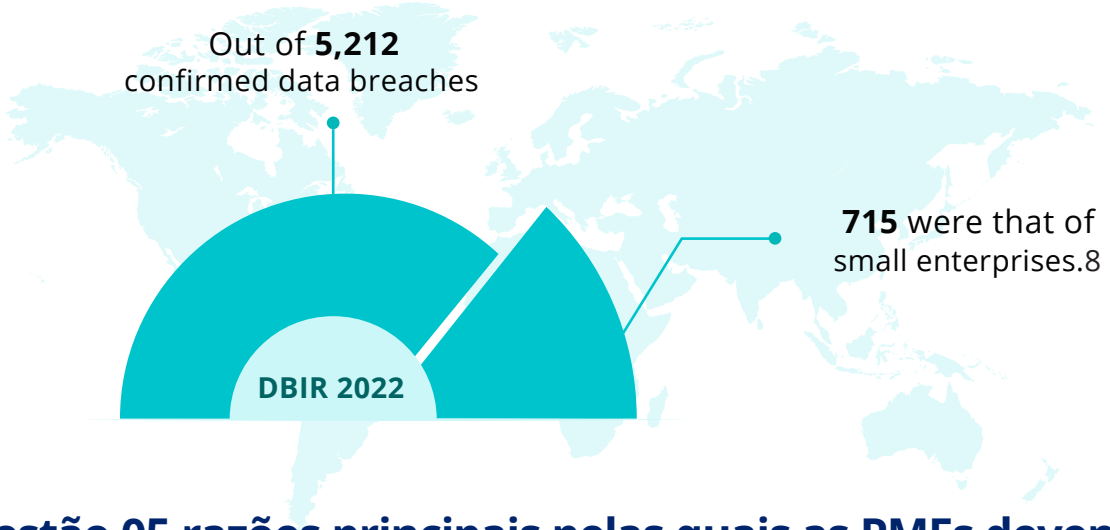
Por que as PMEs são propensas a ataques cibernéticos?

Hoje, as pequenas e médias empresas (PMEs) respondem por 90% de todas as empresas e são cruciais para a economia de um país, especialmente nos países em desenvolvimento. Elas respondem por 70% dos empregos e geram sete em cada 10 postos de trabalho no mercado, no mundo. Como resultado de sua capacidade de criar empregos com custos de capital mínimos, o número de PMEs vem crescendo nos últimos anos.

Devido ao seu impacto, as PMEs têm espaço mínimo para incidentes de segurança cibernética disruptivos. As PMEs que são atacadas pagam o preço de operações interrompidas, pagamentos de resgate, danos à reputação, perda de clientes e uma recuperação longa e difícil. PMEs que se recuperam são relativamente incomuns; quase dois terços das pequenas e médias empresas fecham seis meses após serem invadidas.

> ***"Quando se trata de proteção de dados, as pequenas empresas tendem a estar menos preparadas. Eles têm menos para investir para acertar. Eles não têm equipes de conformidade ou responsáveis pela proteção de dados. Mas as pequenas organizações geralmente processam muitos dados pessoais, e os riscos de reputação e responsabilidade são igualmente reais."***
>
> **Elizabeth Denham,**
> **Ex-comissário de informação do Reino Unido**

As empresas agora enfrentam uma luta mais difícil contra o cibercrime, à medida que mais e mais funcionários optam por trabalhar em casa. O trabalho remoto contribuiu drasticamente para o aumento de ataques bem-sucedidos de ransomware, já que os funcionários agora lidam com os dados da empresa enquanto estão fora das instalações da empresa.



Aqui estão 05 razões principais pelas quais as PMEs devem ser extremamente cautelosas com ataques cibernéticos:

Elas são alvos mais fracos do que empresas maiores

Elas podem não ter uma equipe de TI especializada

Elas agem como uma ponte para as empresas maiores

Não podem pagar pentesters devido à alta demanda e custo

Sua prioridade é P&D e marketing sobre segurança

"90% de todos os CVEs descobertos em 2021 até agora podem ser explorados por invasores com habilidades técnicas limitadas."

Análise NIST NVD,
Laboratórios Redscan

Melhores práticas para uma boa higiene cibernética

O oposto de segurança não é insegurança, é comodidade. A conveniência de fazer coisas fáceis em vez das coisas certas.

Os cibercriminosos de hoje são bons em encontrar redes subprotegidas e desprotegidas. As PMEs devem fortalecer sua postura de segurança. O termo "postura de segurança" refere-se ao programa geral de segurança cibernética de uma empresa e como ela está bem posicionada para enfrentar as ameaças atuais e futuras. Por mais tediosas que sejam as práticas de cibersegurança, incidentes acontecem quando menos esperamos.

Educação do usuário final

Uma corrente é tão forte quanto seu elo mais fraco, e uma organização é tão segura quanto seu funcionário menos consciente. É importante que sua equipe saiba o papel que desempenham na proteção da organização. Eles devem receber treinamento e educação sobre como gerar senhas seguras, detectar golpes de phishing e o que fazer se encontrarem algo suspeito.

Controle de acesso

Em um estudo, 74% das vítimas de violação de dados admitiram que os incidentes cibernéticos envolviam acesso a uma conta privilegiada. À medida que os funcionários mudam de emprego ou departamento, é fácil perder o controle dos privilégios administrativos. Uma conta comprometida com acesso desnecessário a dados confidenciais pode servir como uma entrada fácil para pessoas mal-intencionadas.

Higiene da senha

As credenciais do usuário estiveram envolvidas em mais da metade de todas as violações em 2021. As senhas ainda servem como o principal modo de defesa contra roubo de dados. Use senhas longas que combinem caracteres maiúsculos, minúsculos, numéricos e símbolos. Nunca repita as senhas e seja criterioso ao digitá-las. Combine suas senhas com formas adicionais de autenticação para tornar mais difícil para alguém obter acesso indesejado.

Autenticação

Autenticação é o processo de verificar se um usuário ou dispositivo é quem ou o que afirma ser. É uma parte crítica da higiene cibernética e as organizações podem escolher entre vários tipos de autenticação. O método de autenticação mais óbvio é um nome de usuário e uma senha forte ou PIN. Outra opção infalível é a autenticação multifator (MFA), em que códigos únicos são gerados para o telefone ou endereço de e-mail do usuário. É um método testado e comprovado de aumentar a segurança porque nega acesso a hackers que podem ter apenas suas credenciais de login. A autenticação biométrica usa identificadores biológicos, como reconhecimento facial ou de impressão digital. Outros tipos de autenticação incluem autenticação baseada em certificado, token e logon único.

Gerenciamento de patches

Vulnerabilidades não corrigidas são os principais vetores de ataque que os grupos de ransomware usam para acessar redes fracas. Em qualquer dispositivo pessoal usado para o trabalho, bem como em qualquer dispositivo da empresa, mantenha o software atualizado com patches de segurança. Usando uma ferramenta especializada como o Endpoint Central, você pode identificar patches ausentes e implantá-los em todos os endpoints da sua rede sem nenhuma intervenção manual.

Uma equipe de cibersegurança dedicada

Ainda que os crimes cibernéticos sejam combatidos com tecnologia, há pessoas por trás da luta. É importante formar uma equipe de profissionais preparados e treinados para enfrentar as ameaças de hoje. Em geral, a terceirização é a opção mais econômica e útil para pequenas e médias empresas. Mas as organizações menores devem considerar alocar um orçamento para formar uma equipe de segurança cibernética que possa investigar continuamente o estado de segurança da rede.

Plano de resposta a incidentes

Crie um plano de resposta a incidentes e implemente-o conforme necessário. Realize análises após cada incidente ou simulação para informar sua equipe, fortalecer sua rede e aprimorar respostas futuras. Por último, mas não menos importante, avalie o sucesso da capacidade de sua rede de sustentar a resiliência digital usando métricas que rastreiam mais do que apenas o quão ocupadas suas equipes cibernéticas estão, mas também medem sua eficácia.

Ferramenta moderna de proteção de endpoint

Qualquer software pode ser armado. Veja o malware, que é escrito usando a mesma linguagem de um software útil, mas com intenção maliciosa. Atualmente, o malware pode causar sérios danos, como vazamentos de dados ou falhas na rede. Como os endpoints são os pontos de entrada mais fáceis para os invasores, as empresas devem ter uma proteção robusta para os endpoints. Com o Endpoint Central, as PMEs podem monitorar e proteger seus endpoints enquanto mantêm os custos baixos. Para pequenas empresas com menos de 50 endpoints, este software é totalmente gratuito.

A ferramenta que as PMEs adoram usar

Segundo especialistas, 95% das PMEs admitiram não ter as soluções de tecnologia certas para detectar um ataque cibernético ou ameaça em sua rede. Muitos achavam que havia muitas tecnologias, que eles lutavam para integrar.

Nós concordamos! O uso de uma solução de proteção de endpoint não deve acarretar o custo de lidar com 10 tipos diferentes de software, que podem até não ser compatíveis entre si. É aqui que o Endpoint Central pode ajudar. Tem as capacidades de 10 softwares diferentes em um. O Endpoint Central não apenas ajuda você a obter visibilidade em tempo real para ativos físicos e digitais, mas também ajuda a gerenciar seus endpoints desde a integração até a desativação, em espaços de trabalho híbridos e ecossistemas de sistemas operacionais altamente heterogêneos - tudo em um único console!

O Endpoint Central é amado por pequenas e médias empresas por causa de sua extrema acessibilidade, riqueza de funcionalidades e design fácil de usar. Ele também não requer extensas habilidades de codificação, o que o torna perfeito para organizações que não podem contratar especialistas em TI. O uso deste software também o ajudará a se preparar para a conformidade com os padrões regulatórios. O reconhecimento da IDC, Gartner® e Forrester ano a ano valida o fato de que o Endpoint Central está fazendo a coisa certa!

QUERO SABER MAIS