e-Book

Transformação Digital

CUIDADOS COM A SEGURANÇA DA INFORMAÇÃO NA PEQUENA EMPRESA

SEBRAE

Proteja o seu negócio! Confira algumas dicas para evitar invasões e fraudes pela internet

Ser um(a) empreendedor(a) é um desafio permanente. A todo momento você tem que resolver questões de fornecimento, logística, gestão de pessoas, administrativas, legais... E tudo é importante, disputando seus recursos mais valiosos: tempo e atenção.

A tendência, claro, é priorizar o que traz resultados mais imediatos para o negócio. E, assim, muitas vezes terminamos deixando de lado temas que, naquele momento, não pareciam urgentes. Mas são estratégicos.

Um deles é a segurança da informação, cada vez mais vital por conta do crescimento da dependência das empresas em relação à tecnologia. Ainda mais a após a aprovação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção dos Dados Pessoais (LGPD), que exige das empresas muita atenção no manejo de informações sobre clientes e fornecedores.

Acontece que a segurança das informações tende a ser subestimada por muitos empresários, seja pela falta de conhecimento ou por uma avaliação errada dos riscos que um ataque pode provocar à operação do negócio. Não se engane: esse é um perigo que ronda qualquer empresa, independentemente do tamanho ou visibilidade.

Hackers: a grande ameaça

Hoje, a maior ameaça on line para as empresas e órgãos públicos são os ataques ransomware, nos quais hackers assumem o controle de computadores, bloqueando o acesso a dados e sistemas.

Os ransomwares representam mais da metade dos ataques cibernéticos realizados em todo o mundo. Os hackers utilizam técnicas de engenharia social conhecidas como phishing, a partir de e-mails ou websites construídos especialmente para induzir os usuários a clicar em links maliciosos. Quando o usuário clica, aciona programas que liberam o acesso ao computador e os criminosos podem capturar senhas de sistemas corporativos, de contas bancárias, servidores e todo tipo de dados.

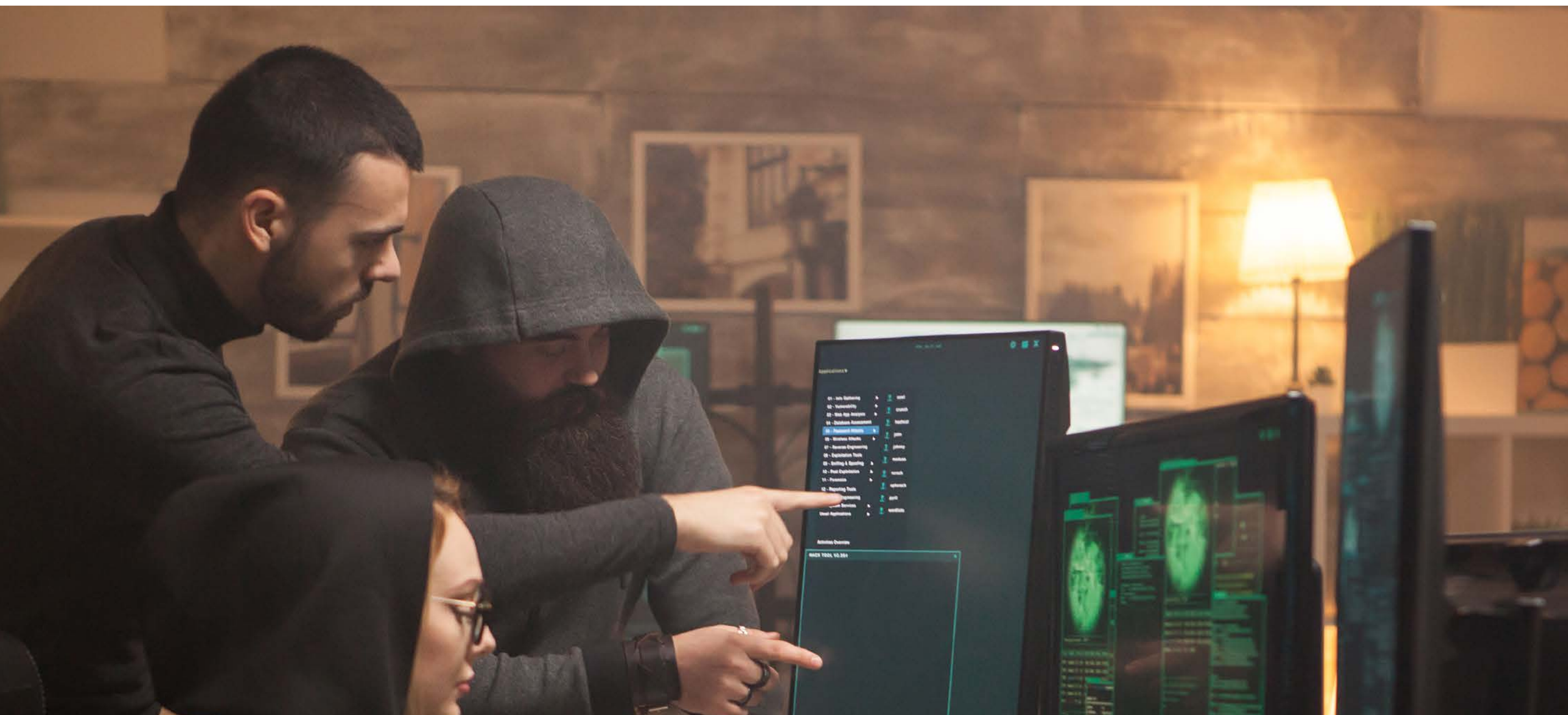
A partir do momento em que ganham o controle dos computadores, os hackers criptografam os conteúdos dos discos rígidos, bloqueando o acesso da empresa aos seus sistemas e dados. E, então, exigem resgates altos para devolver seu acesso. Os resgates são cobrados normalmente em criptomoedas, o que dificulta a identificação dos cyberpiratas.

Se, nas grandes corporações, uma ação de ransomware pode paralisar as operações por dias ou mesmo semanas, em pequenas e médias empresas ela tem potencial simplesmente para quebrar o negócio.

Quem são os hackers?

Ao contrário do que muitos acreditam, a maioria dos ataques não são feitos por pessoas isoladas, trancadas em quartinhos escuros. Em geral, trata-se de organizações criminosas, privadas ou mesmo patrocinadas por governos hostis, cujo objetivo é obter ganhos financeiros ou praticar a espionagem comercial e industrial.

O risco de ataques ransomware é tão grande, atualmente, que a dúvida não é mais se a empresa vai ser vítima, mas, sim, quando isso irá acontecer. E o grande problema é que muitos empreendedores não estão preparados para enfrentar esse perigo.



Outras ameaças graves

Mas nem só de ransomwares vive o crime cibernético. Outros tipos de ataques, tão ameaçadores, devem estar no radar de todo empreendedor. Confira.

FRAUDES NO E-COMMERCE

Incluem transações com cartões roubados, cartões de familiares ou pessoas próximas, sem autorização. Ou feitas pelo próprio titular do cartão que, após receber o produto, questiona a compra junto à operadora. De acordo com a ClearSale, empresa que trabalha com segurança da informação, em 2021, ocorreram cerca de 6,1 milhões de tentativas de fraudes em todo o Brasil, no valor de R$ 5,8 bilhões, o que representou 1,9% do total de transações.

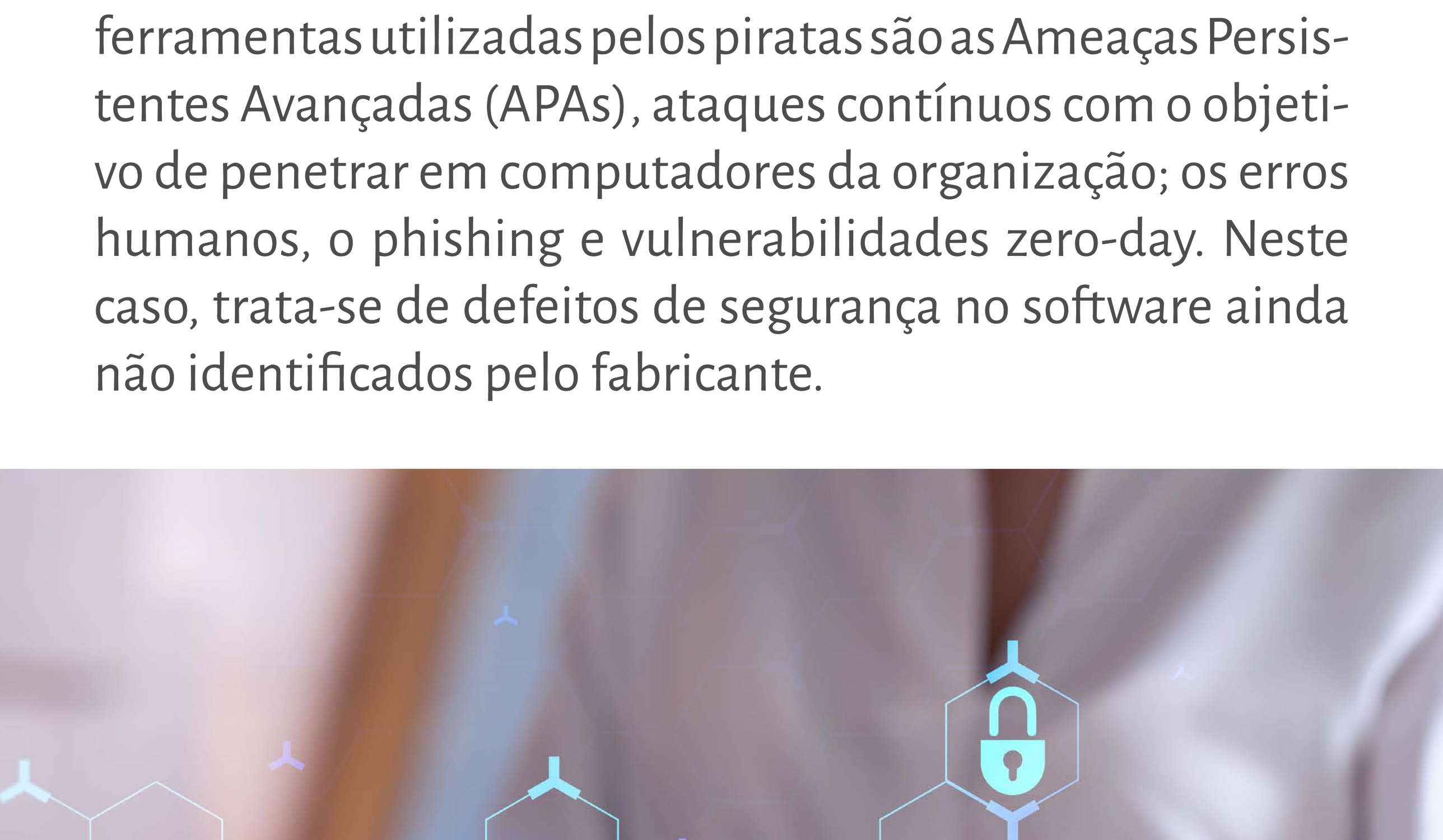
SITES DE E-COMMERCE FRAUDULENTOS

Imitam em detalhes sites legítimos de e-commerce, levando o consumidor desavisado a acreditar que está fazendo uma compra normal, o que afeta a imagem das empresas de varejo sérias. Apenas durante a Black Friday de 2021, o número de sites falsos aumentou em 178% no país, em comparação com a média dos meses anteriores no ano.

ATAQUES À INFRAESTRUTURA DE TECNOLOGIA DA EMPRESA

Além dos ataques de ransomware, um grande perigo são os acessos não autorizados à rede da empresa. Isso ocorre quando alguém de fora consegue entrar nos computadores da organização, aproveitando falhas de segurança em servidores e bases de dados. O que normalmente acontece por falta de atualização do software.

Esses ataques também utilizam malwares – "vírus" introduzidos por programas maliciosos – e aproveitam-se de vulnerabilidades em programas instalados, por conta de falhas conceituais ou desatualização do software. Outras ferramentas utilizadas pelos piratas são as Ameaças Persistentes Avançadas (APAs), ataques contínuos com o objetivo de penetrar em computadores da organização; os erros humanos, o phishing e vulnerabilidades zero-day. Neste caso, trata-se de defeitos de segurança no software ainda não identificados pelo fabricante.



VULNERABILIDADES NO ECOSSISTEMA EMPRESARIAL

Aparecem quando fornecedores, revendedores, transportadoras ou outros elos da cadeia de produção e comercialização da empresa estão vulneráveis ou sofrem ataques cibernéticos que afetam toda a operação. Cada vez mais, pequenas e médias empresas inseridas em cadeias de produção são usadas como porta de entrada para atingir as grandes corporações na ponta final da cadeia, justamente porque estão menos preparadas para enfrentar ataques. Colaboradores trabalhando em casa, a partir de seus próprios computadores – o que cresceu muito durante a pandemia do coronavírus – também são um alvo fácil para os criminosos.

ATAQUES AOS CANAIS ONLINE DA EMPRESA

São invasões aos websites ou às redes sociais do negócio, com a finalidade de capturar dados dos consumidores, redirecionar visitantes para ambientes maliciosos ou inter-ceptar transações comerciais. Uma das táticas é alterar o destino de links em QR Codes, instalando scripts web skimmer em formulários de pagamento para capturar dados de cartões de crédito, ou inserindo encurtadores de URLs com links para sites maliciosos.

Que fazer?

Se você se assustou com o tamanho do perigo, pode ficar um pouco mais tranquilo. Há várias formas de evita-lo ou, pelo menos, de reduzir os riscos. Veja a seguir.

Encare a questão com seriedade. A segurança cibernética deve ser enfrentada com a mesma seriedade dedicada à segurança física das empresas. Na verdade, até mais, já que um cyber ataque pode causar danos maiores do que um assalto ou arrombamento. Afinal, não adianta investir em alarmes, sensores e câmeras sofisticados e deixar toda a operação digital da empresa vulnerável a ataques que podem comprometer a própria sobrevivência do negócio.

DEFINA UMA ESTRATÉGIA SÓLIDA DE DEFESA

Elabore uma política de segurança da informação que determine quais são os processos críticos da empresa, quem pode ter acesso a quais dados ou sistemas, que informações são confidenciais ou não. E restrinja o acesso do pessoal de acordo com seus níveis de autorização.

ELABORE UM PLANO DE RECUPERAÇÃO

E valide esse plano com testes frequentes. Quanto mais bem preparada estiver a organização, mais rapidamente a operação será retomada, em caso de necessidade.

CRIE UM PLANO DE GESTÃO DE CRISE

Caso a empresa sofra um ataque cibernético, é importante estar preparado para comunicar o fato aos colaboradores e outros públicos de interesse. E, também, para apresentar as medidas adotadas com o objetivo de resolver o problema.

CONSCIENTIZE E ATUALIZE SEUS COLABORADORES

O elo mais fraco da segurança está sempre nos usuários internos. É por aí que, normalmente, os hackers ganham acesso aos sistemas. Cada colaborador da empresa, precisa entender claramente o seu papel e o que se espera dele com relação à proteção de dados. Mantenha um canal permanente de comunicação com eles e reveja constantemente cada ocorrência, incluindo as soluções numa espécie de manual de melhores práticas da empresa. Esteja certo de que cada colaborador entenda por que e como proteger os dados do negócio, de acordo com a política traçada.

MANTENHA PADRÕES MÍNIMOS DE SEGURANÇA

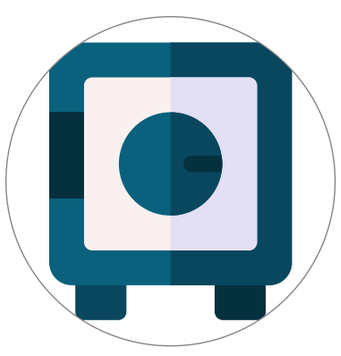
Mantenha um antivírus de qualidade em cada computador e servidor da empresa, protegendo individualmente a máquina contra vírus e malwares. E, também, uma firewall atualizada e configurada adequadamente, que irá funcionar como a principal barreira de proteção entre a rede da empresa e a internet, controlando o tráfego gerado internamente e os acessos externos.

ESCOLHA UMA CONSULTORIA ESPECIALIZADA

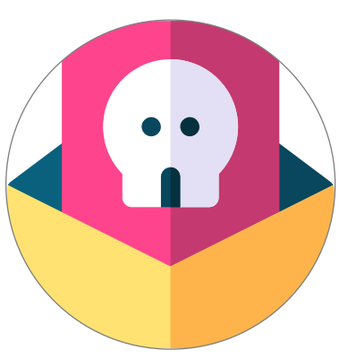
Procure uma empresa de segurança digital confiável para orientá-lo em todo o processo. Pequenas e médias empresas funcionam com equipes enxutas e, mesmo que você tenha técnicos de TI entre os seus colaboradores, a segurança cibernética é um tema específico, multidisciplinar, extremamente dinâmico e que exige dedicação exclusiva. Não improvise: se não puder montar uma equipe de segurança interna, procure ajuda externa.

Medidas imediatas

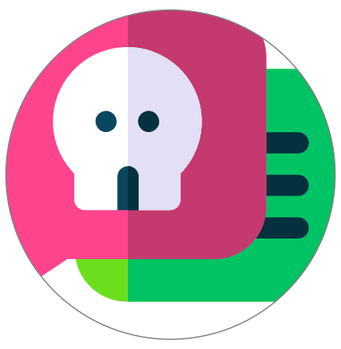
Confira algumas ações que podem ser tomadas de imediato para aumentar o nível de segurança de seu negócio:



Fazer backups constantes dos dados da empresa, incluindo software, firmware, configurações de hardware e software.



Nunca abrir anexos ou clicar em links de e-mails de remetentes que você não conhece. E conscientizar seus colaboradores para que façam o mesmo.



Evitar transmitir nomes de usuário, senhas, dados financeiros e outras informações confidenciais por e-mail, aplicativos de mensagens ou ligações telefônicas.

Criar senhas fortes e não utilizar a mesma senha para várias contas.

Adotar a autenticação de dois fatores, sempre que possível.

Só utilizar redes wi-fi confiáveis e seguras.

AGORA É COM VOCÊ: ESTÁ EM SUAS MÃOS MANTER A EMPRESA FORA DO ALCANCE DOS PIRATAS DA INTERNET!

SEBRAE

Serviço Brasileiro de Apoio às Micro e Pequenas Empresas

0800 570 0800 / www.sebrae.com.br