E-BOOK

CIBERSEGURANÇA SEM MISTÉRIO

PROTEJA-SE NO MUNDO DIGITAL

Evolux

ÍNDICE

INTRODUÇÃO

Ataques cibernéticos são uma ameaça significativa para as empresas, logo, saber como se prevenir é fundamental, para garantir a segurança dos dados dos clientes e a continuidade dos serviços. Esses ataques podem ter consequências devastadoras, como perda ou vazamento de dados confidenciais e indisponibilidade de sistemas, comprometendo gravemente as empresas com prejuízos financeiros e danos à reputação.

Este e-book oferece um guia para proteger sua empresa contra ataques cibernéticos. Abordaremos os tipos mais comuns de golpes, as melhores práticas de segurança da informação e as medidas que você pode tomar para proteger seus dados e sistemas.

TIPOS DE ATAQUES CIBERNÉTICOS

O maior problema dos cibercrimes é a sua discrição. A maioria dos golpes vem com disfarces que, para muitos, são imperceptíveis. Além disso, todos os dias, golpistas criam novos modelos de ataques. Para te ajudar na prevenção, listamos os tipos mais comuns. Confira, a seguir, quais são eles.

1. RANSOMWARE

Este é um dos ataques cibernéticos mais comuns e prejudiciais às empresas. Ele funciona como um **sequestro de dados**, em que o criminoso consegue acessar um sistema ou informações da empresa e solicita um valor de resgate para devolver o acesso ou os dados.

Mesmo pagando o valor de resgate, há um **grande risco de vazamento das informações**, o que é um problema gravíssimo para empresas que trabalham com dados sensíveis.

O criminoso pode conseguir esse acesso por meio de um site ou sistema sem segurança, dentro da rede da empresa, ou ainda, através de anexos de e-mails não confiáveis, baixados inocentemente por membros da equipe.

2. PHISHING

Neste tipo de golpe, são roubados dados importantes como senhas, informações pessoais, conteúdos financeiros, entre outros.

Ele acontece através de armadilhas como envio de links de páginas falsas em que o usuário, achando que é uma página oficial, insere seus dados pessoais ou de login e até realizam pagamentos, achando que estão em um site oficial.

Um caso muito famoso, aqui no Brasil, utiliza o nome do Serasa em anúncios, prometendo limpar o nome da vítima e aumentar seu score. O anúncio direciona para um site falso, praticamente igual ao oficial, e solicita dados da vítima, assim, os criminosos conseguem acessar o perfil dela no Serasa.

Após a coleta de informações pessoais, os golpistas alegam que um pagamento deve ser realizado para dar andamento à demanda. Efetuado o pagamento, os golpistas desaparecem e a vítima só percebe o golpe quando o dano financeiro já foi feito.

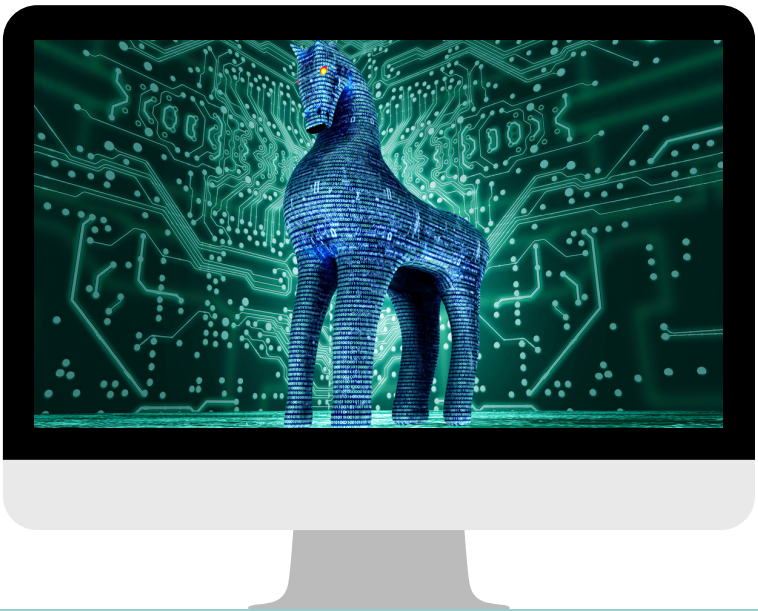
3. CAVALO DE TROIA

Já ouviu a expressão ‘presente de grego’? Pois bem, neste tipo de ataque, os criminosos se inspiram na estratégia utilizada pelos gregos na Guerra de Troia.

O golpe consiste em enviar um “presente” com algo danoso inserido (vírus), que será instalado no computador sem que a vítima perceba.

Geralmente, chega por e-mail, com anexo para a pessoa baixar, ou através de um link, em algum site malicioso, para a pessoa clicar.

Os prejuízos vão desde perda de arquivos até o acesso a informações confidenciais.



4. SPOOFING

Esta prática falsifica a identidade de uma empresa ou pessoa. Isso pode acontecer de diversas formas como presencialmente, por telefone, através de um site falsificado ou e-mail.

O usuário malicioso induz a vítima a pensar que a mensagem veio de uma fonte confiável e a leva a clicar em algum link malicioso ou a informar dados sensíveis.

Para evitar cair nesse golpe, sempre cheque o endereço de e-mail e os dados da fonte da mensagem suspeita que você recebeu.

Se, em sua caixa de entrada, você estiver recebendo mensagens de e-mails, que você nunca enviou, com falhas na entrega (*Failure Notification*), este é um forte indício de que seu e-mail foi invadido e alterado.

Provavelmente, os seus contatos estão recebendo **e-mails falsos em seu nome**. Mude sua senha imediatamente caso isso aconteça, além de habilitar a autenticação multifator.

5. BACKDOOR

Este ataque se parece com o Cavalo de Troia. Porém, nessa modalidade, o criminoso é capaz de **ter acesso administrativo aos arquivos do computador**. Assim, ele poderá ver, deletar e instalar documentos. Além disso, poderá utilizar a imagem da empresa para enviar e-mails ou links com malwares.

COMO PROTEGER A SUA EMPRESA?

Existem várias estratégias que podem ser adotadas para prevenir as empresas de ataques cibernéticos.

Antes de qualquer coisa, as organizações que manipulam dados sensíveis de clientes e parceiros precisam ter a consciência de que **investir em segurança da informação é fundamental** para evitar transtornos dessa natureza.

Confira, a seguir, as principais estratégias de proteção.

FIREWALL

Investir em um **antivírus de qualidade** evita a maior parte dos ataques causados por falha humana, como clicar inocentemente em um link malicioso ou abrir um anexo infectado. Isso porque o Firewall identifica facilmente os arquivos danosos e os elimina.

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

É importante que uma empresa documente suas políticas de segurança da informação, deixando claro para todos os colaboradores quais são as regras estabelecidas na organização.

As políticas variam de acordo com a realidade de cada empresa, mas, no geral, incluem orientações como:

- regras de senhas seguras
- controles de acessos
- gestão de incidentes
- backup de dados
- gerenciamento da estação de trabalho
- gestão de ativos

CONSCIENTIZAÇÃO DA EQUIPE

Como boa parte dos ataques cibernéticos ocorrem por erros internos, é imprescindível que os colaboradores da empresa tenham **treinamentos constantes sobre segurança da informação.**

Portanto, conhecendo as possíveis ameaças, seguindo os métodos de prevenção e as orientações das políticas de segurança da informação, fica mais difícil cair em golpes e cometer falhas de segurança.

ATUALIZAÇÕES REGULARES

Manter os softwares sempre atualizados é uma boa prática de segurança para as empresas. Essas atualizações periódicas corrigem vulnerabilidades identificadas, protegendo, assim, os dados da empresa.

BACKUPS REGULARES

É interessante inserir backups regulares na programação da empresa, para minimizar danos em caso de invasão e indisponibilidade de dados.

VIRTUAL PRIVATE NETWORK (VPN)

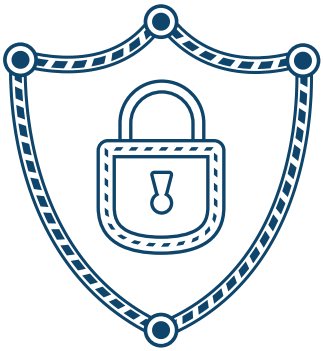
Utilizar uma VPN protege sua rede criptografando todo o tráfego de internet.

A criptografia impede que hackers visualizem informações confidenciais. Isso é ainda mais importante quando uma rede WiFi pública é utilizada, pois é mais fácil para os criminosos monitorarem este tipo de conexão.

A VPN garante que, mesmo que alguém roube seus dados, não consiga decifrá-los.

CONTROLE DE ACESSO

Implementar políticas rigorosas de controle de acesso, como autenticação multifator, restrições de usuários e revisões periódicas de permissões de acesso é essencial para evitar vazamento de dados sensíveis.



ESCOLHA BEM SEUS FORNECEDORES

Contar com parceiros e fornecedores que também se preocupam com a segurança da informação é fundamental para garantir a segurança dos dados da sua empresa.

De nada adianta todo esforço que sua equipe dedica em manter a segurança, se os fornecedores de softwares, aplicativos e outros serviços não se previnem da mesma forma, não é mesmo?

Portanto, ao selecionar seus prestadores de serviço procure saber como eles lidam com a segurança da informação e se possuem certificações de segurança como a ISO 27001.

A ISO 27001 é um padrão internacional de requisitos, processos e normas a serem seguidas para garantir uma gestão de segurança da informação eficaz.

As organizações que possuem esse certificado se mostram mais confiáveis, afinal, estão comprometidas a tratar todos os dados adequadamente.

CONCLUSÃO

De acordo com dados do Serasa Experian, em 2023, ocorreram mais de 10 milhões de tentativas de fraude, a maioria no setor bancário e de cartões (48,1%). O setor de serviços ficou em segundo lugar (30,6%), seguido pelo financeiro (16,3%).

Com tanta exposição ao perigo, é natural que as organizações busquem ampliar suas medidas de segurança. Ao mesmo tempo, esta atitude também é importante para aumentar a confiabilidade da marca perante o mercado, com clientes cada vez mais preocupados com a proteção de dados.

A segurança cibernética é uma responsabilidade contínua.

É importante estar sempre atento às novas ameaças e tomar medidas para proteger sua empresa. Ao seguir as dicas deste material, você pode reduzir significativamente o risco de ser vítima de um ataque cibernético.

Por fim, sabemos que não existe uma 'receita de bolo' para proteger 100% os dados de uma empresa, mas é preciso fazer tudo o que for possível para minimizar as vulnerabilidades e evitar ataques cibernéticos.

É isso que milhares de empresas estão buscando fazer para deixar seus clientes em um ambiente virtual seguro. Você é uma delas?

SEGURANÇA ANTES DE TUDO

Na Evolux, prezamos pela segurança da informação. Por este motivo, adotamos processos rigorosos e constantes para a proteção dos dados de todos que utilizam nossa solução.

Somos uma empresa certificada pela ISO/IEC 27001, um conjunto de normas com padrão internacional para a gestão da segurança da informação nas empresas. Ela estabelece padrões de monitoramento, análise e revisão, focando em melhorias contínuas.

CERTIFIED COMPANY
ISO/IEC 27001
QMS CERTIFICATION

evolux

A certificação ISO/IEC 27001 é concedida para empresas que realizam práticas de gestão da segurança da informação, a fim de garantir a integridade, disponibilidade e confidencialidade das informações em todos os processos realizados na organização.

Para alcançar a certificação, é necessário passar por um processo de adequação aos requisitos normativos, envolvendo todos os setores e colaboradores da empresa. Além disso, é implantado um sólido sistema de gestão da segurança da informação.

Contratar uma organização com a certificação ISO 27001 é ter a tranquilidade de que as informações da sua empresa e de seus clientes estão em um ambiente seguro e em conformidade com as leis e requisitos de proteção de dados vigentes.

Quer conhecer melhor os recursos que o Evolux oferece ao seu atendimento?

Agende uma conversa agora mesmo

5400-0000 comercial@evolux.net.br www.evolux.com.br

evolux