
Como agir
rapidamente
ao sofrer
ataques de
segurança na
empresa?
qriar

Sumário

03 Introdução

04 Por que agir rapidamente?

06 Principais ataques cibernéticos

08 Como agir em casos de ataque?

12 Melhor prevenir do que remediar: como evitar ataques?

14 Qriar

Introdução

Em 2021, o número de ciberataques a redes corporativas no Brasil teve um **aumento de 77%** em relação ao ano anterior. Essa é uma das conclusões do Check Point Research (CPR), feito pela divisão de Inteligência em Ameaças da Check Point Software Technologies.

Além disso, o levantamento também apontou para um **aumento de 50% nos ataques semanais** entre um ano e outro.

Esses dados mostram que as empresas brasileiras estão na mira de hackers, o que exige um preparo maior das organizações para enfrentar esse tipo de problema.

Para que você saiba o que fazer em situações como essa, preparamos esse material que vai servir como um guia na prevenção e na solução da questão. **Continue lendo!**

CAPÍTULO 01

Por que agir rapidamente?

Segundo o ***relatório Cost of a Data Breach da IBM*** referente a 2021, a identificação de um ataque leva um tempo médio de 212 dias e, depois desse período, a contenção do problema ainda pode demorar cerca de 75 dias.

O ciclo de vida completo de uma invasão cibernética é de 287 dias.

Ainda de acordo com esse levantamento, apesar desse tempo de recuperação ser comum, o custo médio para conter um problema desse tipo depois dos 200 dias de ataque foi de 4,7 milhões de dólares. Entretanto, **resolvendo antes dos 200 dias, esse valor caiu para 3,6 milhões.**

Agir rapidamente é DETERMINANTE para a redução de danos.

A IBM, neste mesmo relatório, dividiu os impactos em quatro tipos:

01 **Perda de lucros da empresa —** A média de prejuízo com cancelamento ou não renovação de contratos, perdas de oportunidades de negócio e reputação abalada por conta de um vazamento foi de 1,59 milhões de dólares.

02 **Detecção —** Cerca de 1,24 milhões de dólares foram destinados à identificação e contenção inicial do problema. Esse valor inclui o custo da investigação, gerenciamento de crise e comunicações internas.

03 **Notificação —** O valor destinado a notificação do vazamento a clientes, órgãos reguladores e experts foi de 270 mil dólares.

04 **Responsabilidade Pós-Invasão —** Após a invasão, o custo para adotar medidas exigidas pelos clientes e pagar fianças relacionadas a leis e processos legais foi de 1,14 milhões de dólares.

Por estes motivos, uma resposta rápida a um ataque é essencial para mitigar todos os danos que abalam um negócio após um vazamento. Porém, para não perder tempo e agir de forma realmente eficaz, é preciso “conhecer o inimigo” e entender como ele ataca.

CAPÍTULO 02

Principais ataques cibernéticos

Existem diversos tipos de ataques cibernéticos, mas a maioria deles explora as mesmas vulnerabilidades de um sistema: uma política de senhas fracas, usuários mal informados e falhas em códigos, entre outros.

No entanto, esses tipos de problema poderiam ser facilmente evitados com uma boa estrutura de segurança.

Conheça as principais ameaças a seguir.

RANSOMWARE

Definição: "Ransom", em tradução livre do inglês, significa "resgate". Nesse tipo de ataque, os sistemas e os dados das empresas são criptografados e mantidos como "reféns". Então, para que as informações sejam recuperadas, os invasores pedem um valor em troca.

PHISHING

Definição: Traduzido para "pescaria", neste golpe, os hackers manipulam os usuários para que eles passem as suas informações. Um exemplo comum é o envio de e-mails se passando por organizações, de modo que pareça pessoal e relevante.

BACKDOOR

Definição: Significa "porta dos fundos" e é uma espécie de cavalo de tróia. O invasor acessa o sistema por meio de uma vulnerabilidade e o controla remotamente, agindo de maneira silenciosa.

SPOOFING

Definição: Neste golpe, há a falsificação de endereços de IP, DNS ou e-mails da empresa. Dessa forma, o hacker se passa pela organização para roubar dados de clientes, usuários e funcionários.

DECOY

Definição: No Decoy, o hacker simula um programa legítimo, enganando o usuário, fazendo-o com que ele o utilize como se fosse o verdadeiro. Dessa forma, ele consegue informações de logins, senhas e outros dados.

ZERODAY

Definição: O ataque conhecido como Dia Zero procura por falhas ou bugs que ainda não foram resolvidos em programas e aplicativos recém lançados.

DoS

Definição: No golpe DoS, os hackers enviam uma enorme quantidade de pedidos e solicitações para o sistema da empresa, que fica sobrecarregado, não consegue suportar e sai do ar.

MAN-IN-THE-MIDDLE

Definição: Chamado de "homem no meio", nesse ataque, o invasor se insere na comunicação entre a empresa, um cliente de confiança específico e um servidor. Assim, ele consegue substituir o IP do usuário por um falso e roubar informações.

CAPÍTULO 03

Como agir em casos de ataque?

Uma pesquisa realizada nos Estados Unidos pela empresa americana ***Varonis***, mostrou que cerca de **56% dos entrevistados não saberiam o que fazer em caso de um vazamento de dados.**

Esse número é preocupante porque, sem ter ideia de como agir, a resposta ao ataque demora muito mais, o que **eleva muito a gravidade das consequências da invasão** — como já visto no capítulo anterior.

Por este motivo, é muito importante que a sua empresa tenha um **plano de contingência** em caso de ataques desse tipo. Tendo um protocolo de ação, a resposta de organização será mais rápida e assertiva.

Normalmente, esse planejamento é dividido entre ***pré e pós ataque***.

No ***pré***, a empresa deve considerar **medidas preventivas que antecipem riscos e nem deixem a invasão chegar a acontecer.** No ***pós***, precisa pensar em **quais ações imediatas são capazes de minimizar os impactos.**

UM PRÉ-ATAQUE FORTE E EFICAZ EVITA A NECESSIDADE DE USO DO PÓS

Por isso, ao estruturar o seu **plano de ação para ataques hackers**, considere essas dicas fundamentais.

ADOTAR UM SISTEMA DE MONITORAMENTO ATIVO

A sua resposta a um ataque deve começar assim que ele for detectado. Por este motivo, o seu primeiro investimento deve ser um **bom sistema de *monitoramento de redes* e endpoints,** que identifique e aponte movimentos incomuns.

ISOLAR O SISTEMA

Após ter a noção de que o seu sistema está sob ataque, para mitigar os danos e reduzir os impactos, o primeiro passo é **isolar a parte infectada.** Comece cortando o acesso à Internet e aos servidores, por exemplo. Isso vai diminuir a superfície de ataque e evitar que o vírus e o invasor se espalhem.

ALTERAR SENHAS

É muito comum que os usuários utilizem a mesma senha para diferentes sistemas e plataformas. Isso facilita o trabalho dos hackers, porque, ao **ter acesso a uma password, eles conseguem entrar em tudo.** Por isso, uma boa prática para diminuir os impactos de um ataque é renovar todas as senhas.

TER UM PLANO DE CONTINUIDADE DE NEGÓCIO

Como visto acima, um dos grandes motivos de perda financeira durante ataques hackers é a impossibilidade de realizar negócios, seja pela perda de dados ou pela indisponibilidade de sistemas. Por isso, é f**undamental que você tenha um plano B nesses casos,** com um servidor extra e backups de dados.

TER UMA POLÍTICA DE BACKUP

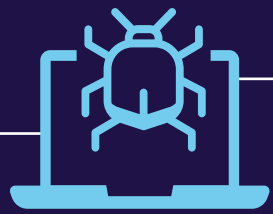
Uma política de backup é a **única coisa que vai te salvar caso nenhuma das opções para restauração funcione,** pois, nesse caso, mesmo que você apague o sistema e retome as configurações de fábrica, os seus dados e informações ainda estarão a salvo. Portanto, a sua ***solução de backup*** deve contemplar a capacidade de armazenamento necessária, a janela de tempo para retenção, as versões dos arquivos, entre outros fatores.

NOTIFICAR AS AUTORIDADES

Após tratar o problema internamente para reduzir os danos, é necessário notificar as autoridades sobre o ocorrido. Nesses casos, pode ser necessário arcar com algumas consequências legais, especialmente se a sua empresa não estava tomando as medidas preventivas adequadas — é o caso da ***LGPD***, por exemplo.

IDENTIFICAR CAUSAS

Uma vez que a situação já estiver "sob controle", vale a pena investigar os motivos do ataque e as vulnerabilidades que foram exploradas. É hora de aprender com os erros e entender o que poderia ter sido feito diferente, para, então, começar a investir em medidas de segurança.



MAPEAR IMPACTOS

Durante todo esse processo, é fundamental analisar os riscos e impactos gerados, porque, em algum momento, a sua empresa terá de lidar com eles — seja por conta de cobrança dos clientes e parceiros, seja devido às obrigações legais. Por isso, vale mapear para ser proativo e oferecer soluções.

CAPÍTULO 04

Melhor prevenir do que remediar: como evitar ataques?

Até este momento do material, todos os dados apresentados confirmam: **a prevenção é melhor do que a remediação.** Trabalhar com soluções que evitem o ataque tem um custo-benefício infinitamente maior do que lidar com as consequências de uma invasão.

Inclusive, o relatório Cost of a Data Breach da IBM também mostrou que, mesmo nos casos em que ataques acontecem, **o prejuízo é muito menor para aquelas empresas que têm sistemas de segurança mais consolidados.**

Organizações com um sistema de segurança completo, inteligente e automatizado levam cerca de 184 dias para identificar uma invasão. Empresas que não têm precisam de 55 dias a mais.

Em empresas não adeptas do Zero Trust, a média de prejuízo é de 42,3% a mais do que em organizações que adotam o conceito.

Sendo assim, em qualquer cenário, com ou sem invasão, ter uma boa estrutura de cibersegurança é sempre a melhor opção.

Veja algumas das soluções que não podem faltar no seu negócio!

SIEM

O SIEM é uma solução que combina gerenciamento de eventos de segurança (SEM – security event management) e gerenciamento de informações de segurança (SIM – security information management). Por realizar essas duas funções, o SIEM é considerado uma das alternativas mais completas para **monitoramento de ameaças e incidentes, gerando relatórios e análises em tempo real.**

PAM

O Privileged Access Management (PAM) é uma ferramenta de ***gerenciamento de acessos privilegiados***, ou seja, ela garante que os usuários certos tenham os acessos corretos no momento em que for necessário. Dessa forma, há uma diminuição dos riscos em relação ao compartilhamento e ao roubo de credenciais.

SOLUÇÃO DE BACK-END BLINDADO

Essa é uma solução que **monitora todas as ações envolvidas nos compartilhamentos de credenciais** de aplicações mais críticas por meio de gravações de sessões e logs. Assim, há o registro e a auditoria das atividades realizadas em tempo real e ainda é feita a análise de comportamentos e detecção de ameaças.

Essas são algumas das soluções essenciais para começar a estruturar um bom plano de contingência de ataques hackers na sua empresa. A Qriar tem muitas outras ferramentas que também auxiliam neste processo para tornar o seu planejamento de proteção mais eficaz, forte e seguro.

Qriar

A Qriar Tecnologia é uma empresa brasileira de cibersegurança e parceiros autorizados dos maiores fornecedores de produtos de cybersecurity do mundo. Oferecemos soluções para conectar pessoas, dispositivos, informações e propósitos de maneira segura.

Atualmente, trabalhamos não apenas fazendo a revenda desses serviços, como também ajudando na implementação dessas ferramentas de maneira personalizada para o seu negócio.

Entre em contato com a Qriar e veja como podemos ajudar a proteger a sua empresa!

Desenvolvido por: agência|mestre