qriar

10 alertas de cibersegurança para proteger sua empresa em 2023: aprenda com cases reais

Os casos recentes de grandes empresas e órgãos governamentais vítimas de ataques cibernéticos são um grande alerta sobre a importância do investimento em soluções de cibersegurança.

A seguir, você verá um panorama desse mercado, as tendências para os próximos anos e **como proteger sua empresa da ação de cibercriminosos.** Confira!

Panorama da Cibersegurança no Brasil

País registrou 31,5 bilhões de tentativas de ataques cibernéticos em 2022

Um levantamento feito pela FortGuard Labs mostrou que o Brasil está entre os países com mais tentativas de ataques cibernéticos em toda a América Latina:

1º MÉXICO **85 BILHÕES**

2º BRASIL **31,5 BILHÕES**

3º COLÔMBIA **6,3 BILHÕES**

4º PERU **5,2 BILHÕES**

As principais dificuldades no enfrentamento do problema são o baixo investimento em soluções de cibersegurança e a falta de profissionais especializados. A seguir, veja a lista com 10 dos tipos de ataques mais comuns.

Principais alertas de segurança para 2023

1. Ransomware

Tipo de malware utilizado para bloquear o acesso aos dados da vítima. Os cibercriminosos costumam pedir resgate sob a ameaça de publicar ou deletar os arquivos.

2. Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS)

Esse tipo de ataque gera sobrecarga nos recursos do sistema, fazendo com que ele pare de responder às solicitações dos usuários, ou seja, os serviços param de funcionar.

3. Man-in-the-middle (MitM)

Um hacker se aproveita de falhas de segurança na comunicação com o usuário para se conectar indevidamente ao servidor. Dessa forma, vão poder interceptar mensagens e utilizar os recursos do sistema como se fosse um usuário confiável.

4. Phishing e Spear Phishing

O cibercriminoso envia e-mails falsos se passando por fontes confiáveis. O usuário tem sua máquina infectada por malware ao clicar em um link ou anexo.

5. Drive-by

Os hackers se aproveitam de sites com falhas de segurança para adicionar scripts maliciosos diretamente no código de uma página. Dessa forma, todos os visitantes ficam expostos à instalação de um malware ao acessá-la.

6. Ataques de senha

Os invasores usam diversos métodos para obter senhas de acesso aos sistemas. O risco aumenta quando não há algum tipo de criptografia e os usuários não são treinados para definir senhas fortes.

7. Injeção SQL

O atacante manipula bancos de dados em SQL e insere comandos para ler, modificar ou deletar a base.

8. Cross-site scripting (XSS)

O cibercriminoso injeta código malicioso em uma página web para redirecionar usuários a sites falsos e roubar informações confidenciais, como senhas e números de cartão de crédito.

9. Cryptojacking

O cibercriminoso injeta código malicioso em uma página web para redirecionar usuários a sites falsos e roubar informações confidenciais, como senhas e números de cartão de crédito.

10. Zero Day

Explora vulnerabilidades de segurança em softwares que acabaram de ser lançados, ou seja, quando os desenvolvedores ainda não tiveram tempo de corrigi-las.

Ataques cibernéticos que tiveram grande repercussão em 2022

Crimes virtuais geraram perdas em empresas de grande porte e órgãos governamentais. Veja alguns dos casos de maior destaque no Brasil.

Americanas e Submarino

Os dois sites de e-commerce gerenciados pela B2W ficaram vários dias fora do ar por conta de uma invasão. A consultoria Economatica estimou que a companhia tenha perdido quase R$ 2 bilhões na Bolsa de Valores Brasileira. Já a Eleven Financial calculou prejuízos na casa de R$ 50 milhões por dia em vendas.

Ministério da Saúde

A invasão a uma base de dados do Ministério da Saúde fez com que milhões de cidadãos tivessem suas informações roubadas, incluindo nomes, endereços e números de CPF. O ataque, cuja autoria foi assumida pelo "Lapsus$ Group", afetou o funcionamento da plataforma ConecteSUS e serviços como a Carteira Nacional de Vacinação Digital.

Record TV

A emissora sofreu dois ataques em menos de uma semana. No primeiro deles, a grade de programação foi prejudicada por vários horas após os sistemas de produção e exibição terem sido sequestrados por cibercriminosos que exigiam o pagamento de um resgate.

Banco PAN

O Banco PAN, controlado pelo BTG Pactual, teve uma de suas bases de dados invadida. Os criminosos copiaram dados cadastrais e informações sobre limite disponível e saldo devedor de clientes.

Quais são os principais desafios para os CISOs em 2023?

Empresas precisam agir rápido para se adaptar às novas regulamentações de privacidade e fortalecer controles de acesso e monitoramento.

Os especialistas da empresa de consultoria em tecnologia Gartner fizeram algumas estimativas que resumem bem os principais desafios dos profissionais de cibersegurança para os próximos anos:

75% da população mundial estará coberta por leis modernas de privacidade de dados até o fim de 2023.

60% das empresas utilizarão os riscos à cibersegurança como fator prioritário para conduzir transações e compromissos comerciais com terceiros.

40% dos conselhos de administração corporativos terão um comitê de segurança cibernética até 2025.

70% dos CEOs exigirão uma cultura de resiliência organizacional para sobreviver a ameaças como crimes cibernéticos, desastres naturais e instabilidades políticas até 2025.

90% será a redução do impacto financeiro causado por incidentes de cibersegurança em empresas que adotarem soluções adaptadas ao contexto do trabalho remoto.

Proteja sua empresa das principais ameaças cibernéticas

Veja algumas das soluções mais apropriadas para se adequar às novas demandas do mercado.

IAM (Identity and Access Management)

Soluções que permitem controlar o acesso a sistemas e recursos digitais com autenticação, autorização e gerenciamento de credenciais de usuários, permitindo a *implementação de uma arquitetura Zero Trust*. Ela é dividida entre três subdisciplinas principais:

- *AM (Access Management)*
- *IGA (Identity Governance and Administration)*
- *PAM (Privileged Access Management)*

Soluções de Segurança para Desenvolvedores

Ferramentas e práticas que ajudam a garantir a segurança do software durante o desenvolvimento, incluindo recursos como testes de segurança automatizados, revisão de código e sistemas de gerenciamento de vulnerabilidades. Entre elas, podemos citar:

- *Secure Digital Access (SDA)*
- *Gerenciamento do Ciclo de Vida e Segurança de APIs, Containers e Micro-serviços*
- *Segurança de Aplicações e SecDevOps*

Soluções de Gerenciamento de Ameaças

Ferramentas que ajudam a proteger sistemas contra ataques e minimizar o impacto deles, caso ocorram. Elas permitem detectar, prevenir e responder a ameaças de segurança por meio de:

- *Gerenciamento de Ameaças e Vulnerabilidades*
- *Monitoramento e Gerenciamento Unificado de Dispositivos*

Sobre a Qriar

Somos uma empresa brasileira especializada na implementação de soluções de cybersecurity.

Time de especialistas certificados

Nossos profissionais contam com a formação necessária e buscam atualização constante para oferecer soluções de cibersegurança alinhadas com as melhores práticas e tecnologias do mercado.

Suporte nas questões técnicas e de gestão

Além de entregar a expertise técnica necessária para lidar com incidentes de segurança, a Qriar ajuda na capacitação da sua equipe e na adaptação dos processos internos.

Reconhecimento das maiores empresas do mercado

Nossa capacidade de entregar projetos robustos é reconhecida por marcas globais do mercado de cibersegurança, como IBM, Micro Focus, Broadcom, Ping Identity e CyberArk.

Conheça as soluções de Cybersecurity da Qriar!

qriar

Desenvolvido por: agência mestre