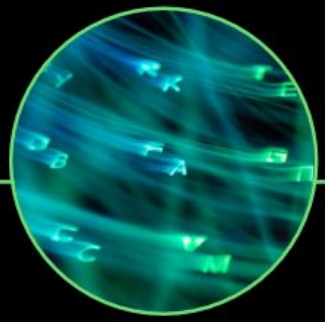
Análise do Ataque Cibernético ao Yahoo em 2013 e suas Consequências

Evandro C. Severgnini
evandrosevergnini@gmail.com

Comprometimento de 3 bilhões de contas de usuários

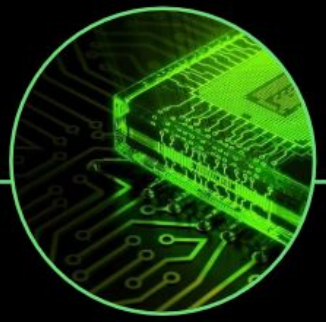


Escala do Comprometimento

O ataque resultou no comprometimento de 3 bilhões de contas de usuários, uma das maiores violações de dados.

Tipo de Dados Expostos

Foram expostos dados sensíveis, como endereços de e-mail, senhas, e números de telefone, comprometendo a privacidade.



Consequências para a Empresa

O Yahoo enfrentou danos significativos à sua reputação e sofreu repercussões legais, incluindo processos judiciais.

Descrição do Sistema Atacado

1

Perfil da Empresa

Yahoo era uma das maiores empresas de serviços online, oferecendo uma ampla gama de serviços digitais.

2

Serviços Disponíveis

A plataforma oferecia e-mail, notícias e mecanismos de busca, atraindo bilhões de usuários globalmente.

3

Armazenamento de Dados

O Yahoo armazenava dados sensíveis de bilhões de usuários, incluindo informações pessoais e credenciais de acesso.

4

Importância dos Dados

Os dados armazenados eram essenciais para a operação da empresa e para a experiência do usuário.

Descrição do Ataque




Método de Ataque

Os atacantes exploraram vulnerabilidades específicas na plataforma para acessar dados confidenciais de maneira ilícita.

Dados Comprometidos

Informações comprometidas incluíram e-mails, números de telefone e perguntas de segurança, aumentando o risco de fraudes.

Segurança das Senhas

Embora as senhas estivessem criptografadas, os algoritmos utilizados apresentavam vulnerabilidades que facilitaram o ataque.

Estratégia dos Atacantes

A estratégia dos atacantes envolveu a exploração de falhas de segurança, indicando uma preparação minuciosa e planejada.

Análise das Vulnerabilidades

1 Quebra de Autenticação

A exploração de falhas no gerenciamento de sessões e autenticação foi um dos principais vetores de ataque.

2 Exposição de Dados Sensíveis

Dados sensíveis estavam sem proteção adequada, permitindo acesso não autorizado e comprometimento de informações.

3 Configuração Incorreta de Segurança

Configurações padrão expostas, como diretórios abertos, facilitaram o ataque e a exploração de vulnerabilidades.

4 Relevância do OWASP

As falhas identificadas se alinham com as diretrizes do OWASP Top Ten, destacando a necessidade de conformidade.