CLOUDFLARE

RESUMO DA SOLUÇÃO

Como uma autenticação forte ajuda a parar ataques de phishing

Chaves de segurança e uma abordagem Zero Trust podem frustrar os phishers

A ameaça imposta pelo phishing

Dados perdidos, redes comprometidas, contas roubadas

Ataques de phishing dirigidos são um dos vetores de ameaça mais perigosos enfrentados pelas empresas hoje. Em ataques de phishing e engenharia social, o objetivo é induzir as pessoas a revelar informações confidenciais ou de acesso. As credenciais de login são os alvos mais comuns.

Quando um ataque desse tipo é bem-sucedido, pode resultar em:

- Invasão de contas
- Um link em um ataque maior à cadeia de suprimentos
- Exfiltração de dados como PII e IP
- Ataques de malware, como ransomware

Felizmente, há soluções muito eficientes disponíveis para diminuir o risco de phishing. Uma das mais importantes é a autenticação multifator (MFA).

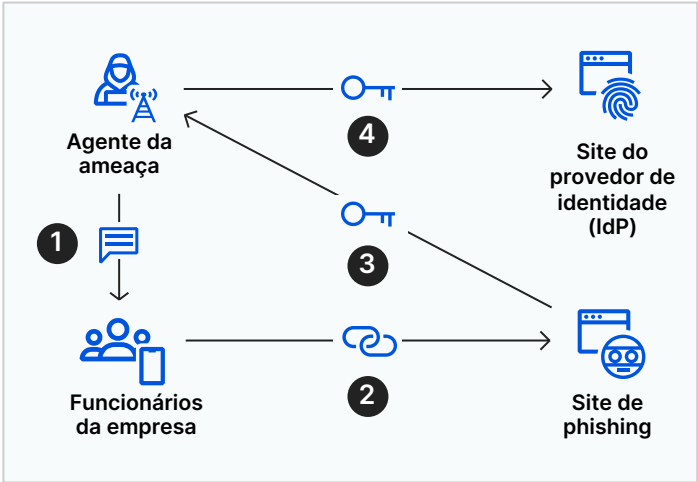


Figura 1: Anatomia de um ataque de phishing por SMS. 1. Uma mensagem de texto que parece legítima é enviada. 2. Essa mensagem é vinculada a um site que também parece legítimo. 3. As credenciais e a senha temporária de uso único da vítima são retransmitidas, em tempo real. 4. Faz login no site do IdP real da empresa.

Como a autenticação multifator (MFA) ajuda a parar o phishing

A MFA neutraliza o roubo de senhas

Com a MFA, é necessário apresentar uma chave, além do nome de usuário e da senha, na hora de fazer login. Sem essa chave, o usuário não consegue acessar a conta, nem o invasor.

MFA com chaves temporárias

É comum a implementação de MFA com chaves temporárias, como códigos temporários de uso único (TOTPs), geralmente enviados por SMS, e-mail ou aplicativos. Embora sejam mais seguras do que a autenticação de um fator, as chaves temporárias podem ser interceptadas por invasores.

MFA com chaves de segurança

Depois de serem emitidas, as chaves de segurança compatíveis com o padrão FIDO2 não podem ser interceptadas por invasores e são quase impossíveis de roubar sem acesso físico. Uma pesquisa do Google descobriu que o uso de chaves de segurança compatíveis com o padrão FIDO2/U2F impediram 100% das tentativas de invasão de conta.[1]

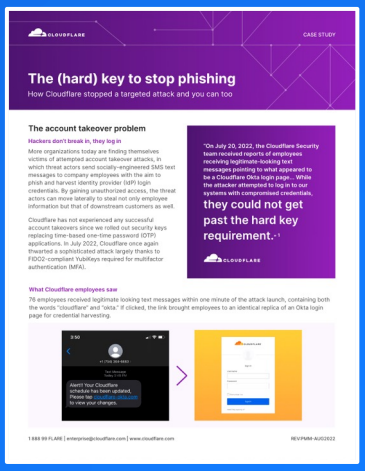
Aplicar a autenticação forte seletivamente

Algumas soluções de IAM são compatíveis com autenticação forte, mas não permitem que os administradores realmente a exijam. Com o ZTNA, é possível garantir que a autenticação FIDO2 seja necessária especialmente para aplicativos que hospedam dados confidenciais. A Cloudflare exige MFA de chave de segurança para cada autenticação, o que fortaleceu fortemente nossa postura de segurança.

"Em 20 de julho de 2022, a equipe de Segurança da Cloudflare recebeu relatos de funcionários que estavam recebendo mensagens de texto que pareciam legítimas e levavam a uma página de login da Okta para a Cloudflare... O invasor tentou entrar em nossos sistemas com credenciais comprometidas,

mas não conseguiu porque era necessário inserir uma chave de segurança." [2]

CLOUDFLARE



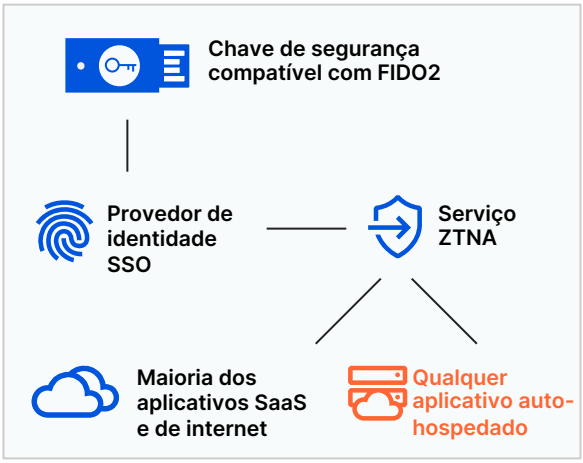
Implemente uma autenticação forte em todos os locais

MFA compatível com FIDO2 para todos os aplicativos

A aplicação de MFA para serviços em nuvem é possível de várias maneiras convencionais, principalmente quando um serviço de logon único (SSO) é usado. Mas isso pode ser difícil com aplicativos herdados ou fora da web, muitos dos quais não suportam esse tipo de autenticação nativamente.

Simplifique a implementação com o ZTNA

O Acesso à Rede Zero Trust (ZTNA) atua como uma camada de agregação para todos os recursos e ativa políticas de autenticação rigorosas para cada um. Aplicativos SaaS, auto-hospedados e fora da web são protegidos pelo ZTNA, o que torna a autenticação forte mais fácil de aplicar em todos os aplicativos.



Principais conclusões para empresas que estão implementando a autenticação forte

1

Centralize seu IAM

Centralize o gerenciamento de identidade e acesso (IAM) para simplificar a implementação do MFA em todos os aplicativos.

2

Aplicar MFA seletivamente

Estabeleça a aplicação seletiva de opções de MFA — somente TOTP e FIDO2 ou FIDO2 — com base na identidade e no contexto.

3

Compatibilidade com dispositivos móveis

Emita soluções FIDO2 para laptops, computadores desktop e servidores, bem como dispositivos móveis.

Acelere seu roteiro Zero Trust

Solicite um workshop sobre arquitetura

Não está pronto para sua avaliação?

Solicite uma avaliação gratuita.

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. Post no blog da Cloudflare em 9 de agosto de 2022, "The mechanics of a sophisticated phishing scam and how we stopped it", blog.cloudflare.com/2022-07-sms-phishing-attacks/