AVALIAÇÃO

Avaliação de riscos: segurança Multi-Factor Authentication (MFA)

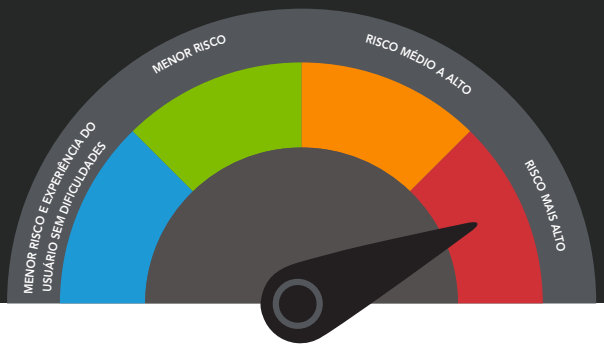
Entenda a escala de risco das soluções de autenticação atuais

80% de todas as violações relacionadas a invasões envolvem credenciais de usuário roubadas ou pouca higiene no cuidado com senhas,[1] e mais de 613 milhões de senhas foram expostas por violações de dados.[2] Adicionar a Multi-Factor Authentication (MFA) como uma camada de segurança de login adicional pode reduzir significativamente o risco, mas a maioria das soluções MFA tradicionais ainda pode ser comprometida com relativa facilidade.

Qual é o grau de maturidade da segurança por autenticação da sua organização? Entenda os riscos dos modelos de autenticação atuais:

Risco mais alto

Autenticação por nome de usuário e senha



As organizações que dependem exclusivamente da força das credenciais para uma autenticação segura são altamente vulneráveis a ataques. Os nomes de usuário e as senhas estão menos seguros do que nunca. As informações de login são roubadas, hackeadas e coletadas por agentes altamente motivados e, em seguida, são rapidamente monetizadas, usadas ou vendidas na dark web.

Como agentes mal-intencionados contornam nomes de usuário e senhas:

- **Credential stuffing**
- **Phishing**
- **Pulverização de senha**
- **Força bruta**
- **Violação de dados anterior/senhas reutilizadas**
- **Redefinição de senha**
- **Keystroke logging (registro por pressionamento de tecla)**
- **Descoberta local**

E o fato de que os usuários tendem a repetir as senhas em vários websites ameaça ainda mais a segurança da empresa; a sua segurança não vai além da conta pessoal menos segura de seus usuários. As vulnerabilidades inerentes até mesmo às senhas mais complexas geradas por algoritmos provam a necessidade da MFA. Em última análise, nunca é aconselhável confiar em um único nível de segurança, a autenticação de fator único neste caso. A melhor segurança da categoria sempre inclui várias camadas de defesa.

Risco médio a alto

MFA (Multi-Factor Authentication) padrão

Adicionar a funcionalidade MFA à sua pilha de segurança de autenticação melhora imediatamente a segurança da empresa. A MFA, incluindo a 2FA (autenticação de dois fatores), exige no mínimo dois fatores de autenticação separados para verificar um usuário. O primeiro fator é normalmente uma senha. O segundo (e possivelmente o terceiro) fator pode ser algo que você sabe, como um PIN ou uma pergunta de segurança; algo que você possui, como um dispositivo, código/senha de uso único ou token físico/digital; ou algo que você é, o que inclui biometria, como impressão digital e ID facial, ou sinais contextuais, como localização.

Embora a MFA tradicional reduza significativamente o risco em comparação com a autenticação de nome de usuário/senha de fator único, ela ainda é vulnerável a vários métodos para contornar a segurança de autenticação:

- **Phishing**
- **Uso de proxies transparentes (ataques MITM [man-in-the-middle])**
- **Interceptação de código de autenticação por e-mail ou SMS**
- **Credential stuffing**
- **Ataques de repetição**
- **Troca de SIM**
- **Engenharia social**
- **Vulnerabilidades em páginas online que lidam com operações de MFA**

Há muitos exemplos bem documentados de agentes de ameaça que contornam a autenticação multifator. Uma violação importante em 2020 foi realizada usando uma combinação de engenharia social e phishing para contornar uma solução de MFA e poderia ter sido evitada com o uso de chaves de segurança físicas.

Menor risco

FIDO2 MFA via chave de segurança física

O FIDO2 é o método de autenticação mais forte baseado em padrões disponível e resolve as vulnerabilidades de segurança da MFA tradicional, eliminando os riscos de phishing, MITM e ataques de repetição. O padrão FIDO2 consiste na especificação de autenticação da Web do World Wide Web Consortium e no protocolo cliente para autenticador correspondente da FIDO Alliance. Este modelo de autenticação permite o futuro da MFA, que é a autenticação por meio de credenciais de login criptográficas que nunca saem do dispositivo do usuário e nunca são armazenadas em um servidor. O FIDO2 também suporta a eventual evolução para autenticação totalmente sem senha.

A desvantagem é que a única maneira de habilitar o FIDO2 MFA é comprar chaves de segurança físicas para cada usuário usar como um fator de autenticação.

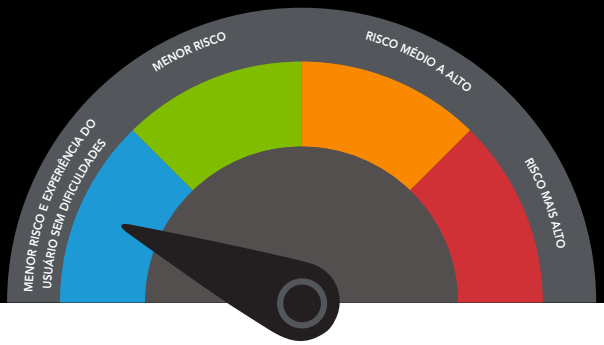
Embora o FIDO2 seja o padrão mais seguro, a implementação por meio de chaves de segurança físicas pode apresentar muitos desafios:

- **Custo de compra e manutenção das chaves para cada usuário**
- **Complexidade da distribuição e do gerenciamento de chaves**
- **Substituição de chaves de hardware perdidas**
- **Incapacidade de atualizar ou corrigir chaves de hardware**
- **Distribuição desigual, pois somente determinados funcionários recebem chaves**

Comprar, configurar, distribuir e gerenciar chaves físicas para todos os funcionários é algo caro e demorado. Além disso, exigir que os usuários conectem uma chave física ao seu dispositivo para cada login reduz a produtividade ao adicionar uma experiência de usuário complexa.

Menor risco e experiência do usuário sem dificuldades

MFA de última geração na edge



O Akamai MFA é uma solução FIDO2 de última geração que apresenta um fator de autenticação à prova de phishing, protegido por criptografia. O serviço utiliza uma aplicação de smartphone no lugar de uma chave de segurança física, resolvendo os desafios que frequentemente impedem as empresas de implementar o FIDO2 MFA. Ele pode ser implantado de forma rápida e fácil usando um smartphone existente, fornecendo o mais alto nível de segurança de autenticação com uma experiência de usuário sem dificuldades. O Akamai MFA elimina o risco de phishing e suporta a eventual evolução para o futuro da autenticação sem senhas.

Saiba mais sobre o Akamai MFA e inicie um trial gratuito de 60 dias aqui: **akamai.com/mfa**.

Fontes:

1. https://www.infosecurity-magazine.com/blogs/pwned-passwords-business-risk/
2. https://haveibeenpwned.com/Passwords

A Akamai protege e entrega experiências digitais para as maiores empresas do mundo. A Akamai Intelligent Edge Platform engloba tudo, desde a empresa até a nuvem, para que os clientes e suas empresas possam ser rápidos, inteligentes e estar protegidos. As principais marcas mundiais contam com a Akamai para ajudá-las a obter vantagem competitiva por meio de soluções ágeis que estendem o poder de suas arquiteturas multinuvem. A Akamai mantém as decisões, as aplicações e as experiências mais próximas dos usuários, e os ataques e as ameaças cada vez mais distantes. O portfólio de soluções Edge Security, desempenho na Web e em dispositivos móveis, acesso corporativo e entrega de vídeos da Akamai conta com um excepcional atendimento ao cliente e monitoramento 24 horas por dia, sete dias por semana, durante o ano todo. Para saber por que as principais marcas do mundo confiam na Akamai, visite www.akamai.com, blogs.akamai.com ou siga @Akamai no Twitter. Nossas informações de contato globais podem ser encontradas em www.akamai.com/locations. Publicado em 03/21.