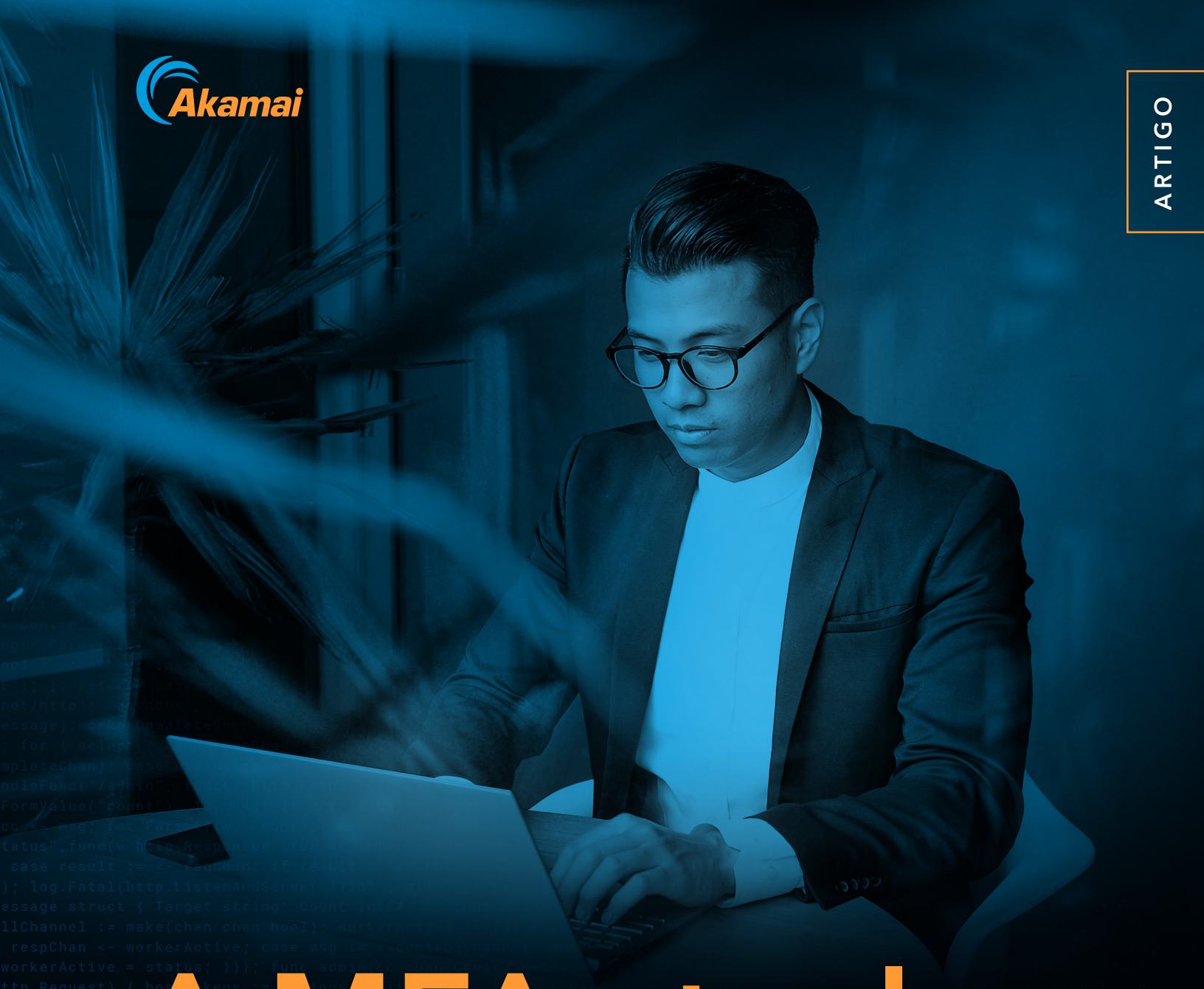
Akamai

ARTIGO



A MFA atual: será uma ilusão de segurança?

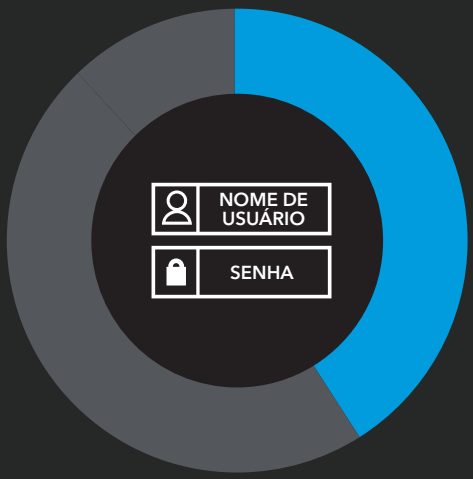
Nomes de usuário e senhas não são suficientes

80% das violações de segurança envolvem credenciais comprometidas.[1] E, embora parte disso seja devido à falta de higiene com as senhas, até mesmo senhas complexas e indecifráveis desenvolvidas por algoritmos podem apresentar problemas.[2] Uma auditoria recente realizada na Dark Web descobriu 15 bilhões de logins roubados devido a 100.000 violações.[3]

A necessidade da conectividade digital, a confiança nos serviços na nuvem e a realidade dos ambientes híbridos, juntamente com a confiança nas senhas, deixam os usuários vulneráveis a inúmeros vetores de ataque de autenticação:

- **Credential Stuffing**
- **Pulverização de senhas e outras estratégias de força bruta**
- **Esforços internos e descoberta local**
- **Phishing e engenharia social**
- **Keystroke logging (registro por pressionamento de tecla)**
- **Proxy malicioso e campanhas de resposta**

E a pandemia global agravou esse cenário, demonstrando a necessidade de acesso seguro em qualquer lugar e em qualquer dispositivo. Ao levarmos em conta que 100% das violações relacionadas a credenciais ocorrem depois que o usuário é autenticado, torna-se evidente que as senhas não são a forma ideal de autenticação.



Embora os pontos fracos sejam conhecidos, 41% das organizações ainda acreditam que nomes de usuário e senhas sejam uma das ferramentas de gerenciamento de acesso mais eficazes.[4]

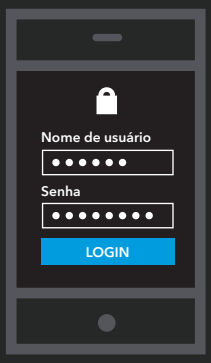
500%

A Akamai descobriu que ataques de phishing, engenharia social, credential stuffing e força bruta estão aumentando. Entre março e maio de 2020, observamos um aumento de quase 500% nos malwares.

Os benefícios da autenticação multifator

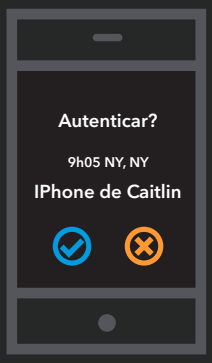
Não é surpresa, portanto, que a tecnologia MFA (Multi-Factor Authentication) esteja se tornando cada vez mais conhecida. Em poucas palavras, a MFA protege sua empresa usando mais de uma fonte de validação para verificar a identidade antes de conceder o acesso.

A MFA requer uma combinação de, pelo menos, duas das três credenciais de autenticação a seguir:



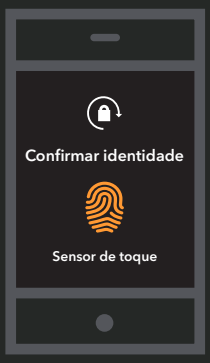
Algo que você sabe

Essa autenticação é baseada em informações. Isso inclui senhas, códigos PIN, respostas a perguntas de segurança ou, até mesmo, pictogramas.



Algo que você tem

Essa autenticação é baseada em token, físico ou virtual. Isso inclui smart cards, controles remotos, senhas de uso único, notificações por push ou códigos SMS enviados ao celular.



Algo que você é

Essa autenticação é contextual ou biométrica. Isso inclui comportamento, sinais de localização ou hora, impressão digital, reconhecimento facial, padrão de voz ou fala, ou uma assinatura.

A implementação de uma solução MFA reduz significativamente o risco de acesso não autorizado e violações do sistema. Na verdade, as organizações que usam a MFA têm 99,9% menos probabilidade de sofrerem invasões do que aquelas que não usam.[5] A MFA possibilita e simplifica o acesso seguro a todos os ambientes: aplicações na nuvem, no local, baseadas na Web, SaaS e IaaS. Uma solução MFA também é um componente essencial na migração da segurança empresarial para estruturas como Zero Trust e SASE.

Ao exigir mais do que apenas nomes de usuário e senhas, unificando a experiência de login e integrando-se a outras ferramentas de segurança nativas da nuvem, as tecnologias MFA também têm o potencial de aumentar a produtividade e a viabilidade do usuário. Além disso, a autenticação gerenciada centralmente atende a muitas questões e requisitos de conformidade.

Mas a MFA tradicional não é tão segura quanto você pensa

Um serviço MFA baseado em push padrão pode ser facilmente manipulado por um hacker para apropriação de contas. Se a segurança das tecnologias MFA atuais não for aprimorada, você estará em risco.

A MFA é uma forma de segurança de perímetro, mas a nuvem e o estilo de trabalho atual não têm perímetro. A MFA não foi projetada para interromper ataques não relacionados a logins. Ela só protege o login no perímetro quando o usuário tenta obter acesso ao sistema. Os cibercriminosos desenvolveram mecanismos de phishing e engenharia social relativamente simples, mas altamente eficazes, para contornar essa realidade.

Considere este cenário:

1. **Como consequência de alguma forma de engenharia social, um funcionário insere um nome de usuário e uma senha reais em um website falso (phishing) configurado por um invasor.**
2. **Ao ter acesso a essas credenciais, o invasor as insere no portal de login real.**
3. **Isso faz com que uma notificação por push seja enviada ao telefone do funcionário.**
4. **O funcionário aceita a notificação por push como um procedimento normal de login.**
5. **O invasor concluiu duas formas de verificação e consegue o acesso.**

Esse é o maior ponto fraco da segurança de uma notificação por push padrão. Qualquer invasor com um conjunto de credenciais roubadas pode fazer com que notificações por push sejam enviadas para o telefone de um funcionário. O que pode evitar que uma violação de segurança interfira na rotina normal de uma empresa é a habilidade de um funcionário de perceber a diferença entre um push legítimo e um golpe. Para que o invasor consiga acesso, o deslize de apenas um funcionário entre vários é o suficiente.

MFA à prova de phishing

Uma solução MFA verdadeiramente segura usa padrões FIDO2. No nível mais básico, isso significa que a segurança é fornecida pela tecnologia em vez de depender das decisões do usuário.

Como isso é feito? Os padrões FIDO2 usam algumas técnicas que impedem o phishing.

Primeiro, a solicitação de autenticação (o desafio de MFA) é sempre enviada para a estação de trabalho que gerou a solicitação de acesso. O navegador dessa estação de trabalho direcionará a solicitação de autenticação para qualquer chave de segurança conectada localmente. Aplicado ao cenário acima: em vez de o invasor obter o serviço MFA para enviar a notificação por push para o telefone do funcionário, agora, o desafio de MFA regressará à estação de trabalho do invasor. Como o invasor não tem a chave de segurança do funcionário, não haverá nenhum tipo de retorno. Uma apropriação de conta será impedida.

Definido: padrões e especificações de autenticação

FAST Identity Online (FIDO) Alliance

O órgão responsável pelo desenvolvimento, o uso e a conformidade com os padrões de autenticação.

FIDO2

O termo abrangente para o mais novo conjunto de especificações de autenticação da FIDO Alliance. Os padrões incluídos na coleção são CTAP1, CTAP2 e WebAuthn. O FIDO2 permite que os usuários utilizem dispositivos comuns para realizarem a autenticação facilmente em serviços online tanto a partir de celulares quanto de computadores fixos.

WebAuthn

Um padrão da Web publicado pelo W3C (World Wide Web Consortium) que é um componente principal do FIDO2. O objetivo do projeto é padronizar uma interface para autenticar usuários em aplicações e serviços baseados na Web usando criptografia de chave pública.

CTAP (Client to Authenticator Protocol)

Uma especificação desenvolvida pela FIDO Alliance que permite a comunicação segura entre um autenticador de roaming (como um smartphone) e um autenticador interno: o cliente ou a plataforma.

Depois, o navegador envia dados para a chave de segurança juntamente com a solicitação de autenticação. Esses dados incluem o nome de domínio da origem que enviou a solicitação de autenticação, conforme visto pelo navegador. Se o invasor simplesmente encaminhar a solicitação de autenticação recebida para a estação de trabalho do funcionário, esses dados conterão o nome de domínio do website de phishing. A chave de segurança reconhecerá a incompatibilidade entre o nome de domínio do website com o qual ela foi originalmente registrada e o nome de domínio que está solicitando a autenticação e se recusará a responder. Mais uma vez, o ataque fracassará.

Se a MFA à prova de phishing é mais segura e é uma possibilidade, por que não é utilizada com mais frequência? As chaves de segurança físicas exigidas são caras e complicadas. Ou eram, até agora.

MFA de última geração na edge

A TI se viu em uma situação de perdas e ganhos ao avaliar e implementar tecnologias MFA. Para ter a melhor segurança, a TI precisa gastar mais para implantar hardware, adquirir chaves de segurança físicas para cada funcionário e gerenciar a distribuição e a operação de todas essas chaves. Ela também deve garantir que cada usuário adote o uso dessa tecnologia de chaves que está longe de ser ideal, pois implica outro hardware para usar e acompanhar.

A alternativa é ter menos segurança e adotar a forma de notificações por push para os smartphones de funcionários, que são convenientes e não agregam custos. Isso explica o motivo de a MFA ser tão utilizada hoje em dia. E também explica por que tantas empresas correm o risco de serem violadas.

Mas a segurança não precisa mais ser trocada por custo e facilidade de adoção.

O serviço Akamai MFA apresenta um novo fator de autenticação. Ele digitaliza a segurança do FIDO2 com apenas um smartphone e um navegador da Web e combina-o com a experiência familiar e de fácil utilização de uma notificação por push, que pode ser usada em qualquer plataforma como autenticador de roaming. E sem exigir chaves de segurança físicas. A solução oferece as funcionalidades mais seguras dos padrões FIDO2 a um baixo custo, com facilidade de instalação e consumo, bem como interoperabilidade com provedores de identidade comuns.

Proteja sua organização contra phishing, credential stuffing e apropriação de contas com o Akamai MFA. Saiba mais sobre a tecnologia MFA da Akamai, a primeira do tipo, e prepare-se para um futuro seguro e livre de senhas.

Saiba mais em akamai.com/mfa.

Fontes:

1. https://enterprise.verizon.com/resources/reports/dbir/
2. https://www.infosecurity-magazine.com/opinions/problem-password-everything-1/
3. https://www.forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime/?sh=27fa6368180f
4. https://www.businesswire.com/news/home/20200616005047/en/Weakest-Link-Prevails-Overreliance-Passwords-Continues-Compromise
5. https://www.hipaajournal.com/multi-factor-authentication-blocks-99-9-of-automated-cyberattacks/