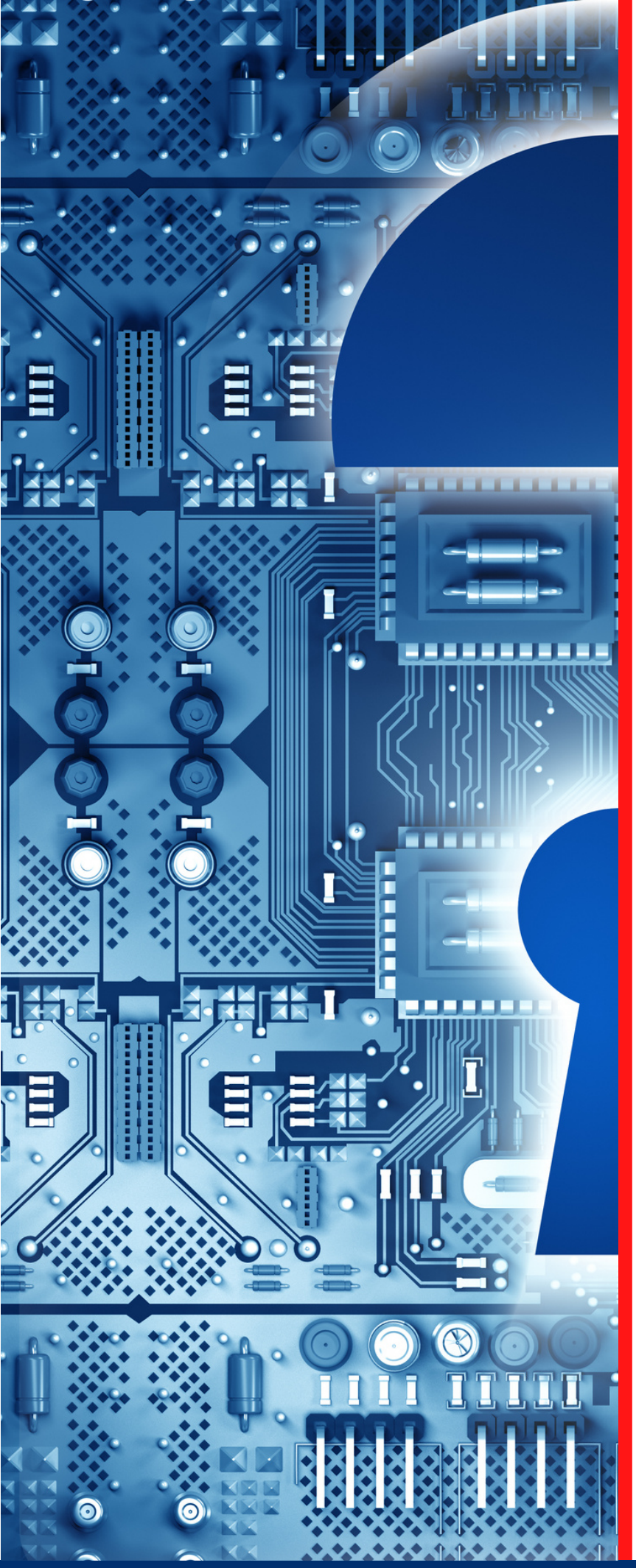


OSIC

ORIENTAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

11/2023

Autenticação Multifator (*Multi-factor Authentication* – MFA) e seus desafios

Textos: João Alberto Muniz Gaspar
Diagramação: Douglas Rocha de Oliveira
Produção: Secretaria de Segurança da Informação e Cibernética

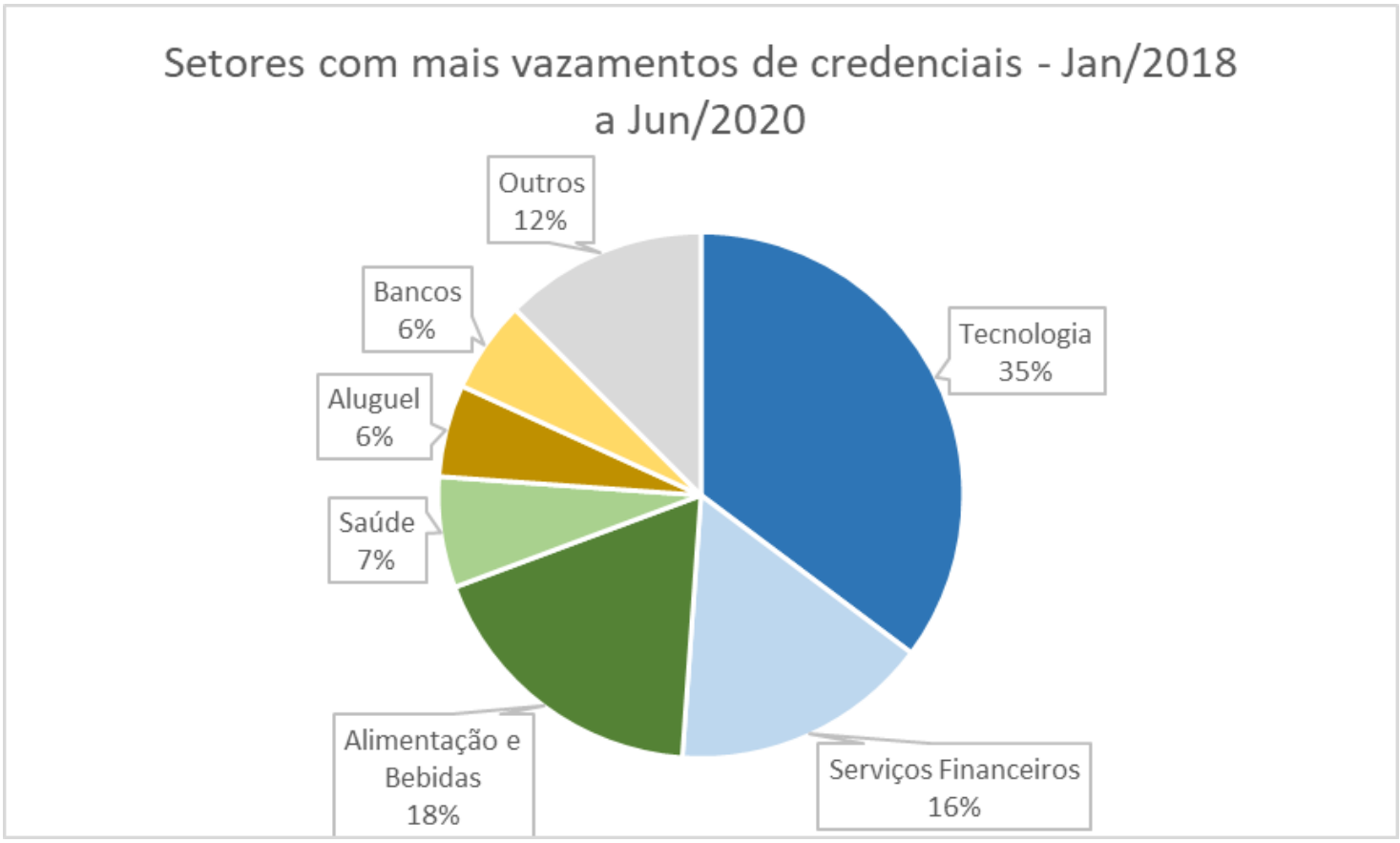
Espaço cibernético inclusivo, seguro, estável, acessível e pacífico.

TLP:CLEAR

Motivação

A incerteza em torno da segurança do uso exclusivo de credenciais de *login* (conta e senha), como forma de autenticação de usuários, não é algo novo. Boa parte de pesquisadores e profissionais em segurança da informação duvidam de sua eficácia há décadas.

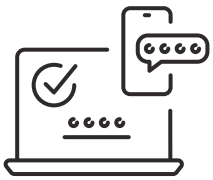
Em 2020, os pesquisadores de segurança cibernética da *Digital Shadows Photon Research Team*, após uma pesquisa de mais de 2 anos, determinaram que foram vendidas na *Dark Web* mais de 15 bilhões de credenciais resultantes de mais de 100.000 vazamentos de dados e publicaram essas descobertas no relatório intitulado *"From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover"* (esta referência está disponível em https://resources.digitalshadows.com/whitepapers-and-reports/from-exposure-to-takeover).



Em 2021, o Brasil ficou no topo de vazamento de informação no mundo, com mais de 227 milhões de dados de brasileiros expostos (https://www.cnnbrasil.com.br/tecnologia/em-2021-brasil-ficou-no-topo-de-vazamento-de-informacao-no-mundo-diz-especialista/).

A existência de enormes repositórios de dados com milhões de credenciais de *login* (*usernames*, *e-mails* e senhas) sendo negociados na *Dark Web* não é uma surpresa para muitos especialistas em segurança. É apenas mais uma prova de que a identidade se tornou o novo perímetro de segurança e o campo de batalha para mitigar ataques cibernéticos que se fazem passar por usuários legítimos.

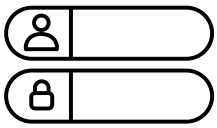
Autenticação Multi-fator (MFA)



Em vez de confiar apenas na autenticação de fator único, ou seja, na autenticação baseada exclusivamente em nomes de usuário e senhas, os profissionais de segurança têm considerado a adição de camadas de segurança adicional para seus controles de acesso, implementando uma autenticação multifator (MFA).

De fato, em 31 de agosto de 2021, a *Cybersecurity and Infrastructure Security Agency* (CISA) incluiu a autenticação de fator único na sua lista de práticas ruins de segurança da informação, (https://www.msspalert.com/cybersecurity-news/cisa-single-factor-authentication-concerns/). A lista de práticas ruins da CISA descreve práticas de segurança que devem ser evitadas por serem consideradas excepcionalmente arriscadas.

De acordo com a CISA,



"O uso de autenticação de fator único para acesso remoto ou administrativo a sistemas que suportam a operação de Infraestrutura Crítica e Funções Críticas Nacionais é perigoso e eleva significativamente o risco à segurança nacional, segurança econômica nacional e saúde e segurança públicas nacionais. Essa prática perigosa é especialmente flagrante em tecnologias acessíveis pela *Internet*. "

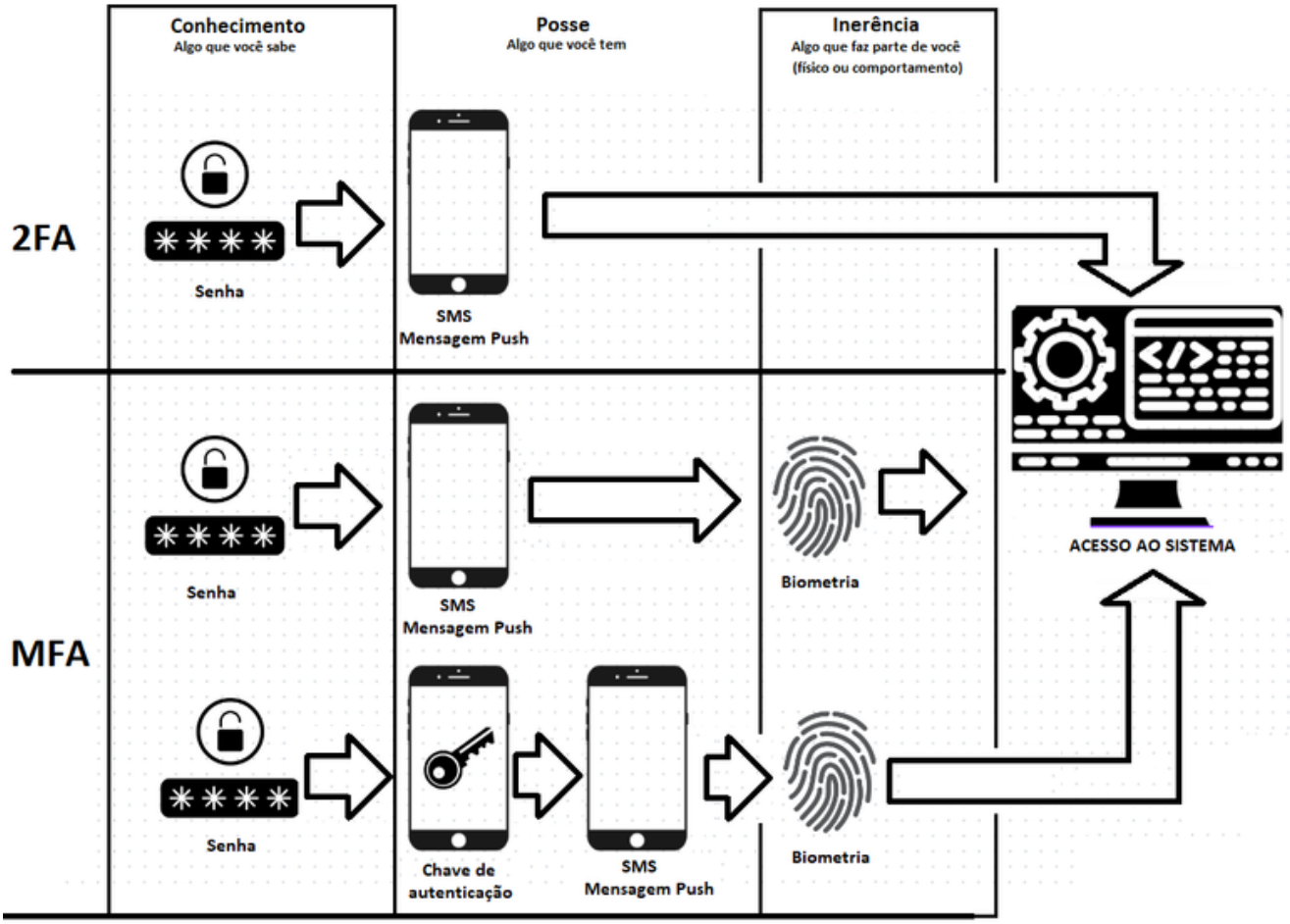
A autenticação multifator (MFA) é baseada em uma abordagem em camadas, com dois ou mais tipos de autenticação. Um dos principais objetivos da MFA é a adição de fatores de autenticação para uma maior segurança no processo.

Os três fatores de autenticação de usuários mais comumente utilizados são:

- Conhecimento: algo do conhecimento do usuário, como uma senha ou uma pergunta pessoal.
- Posse: algo de posse do usuário, como uma chave de segurança ou um *token*.
- Inerência: algo inerente ao usuário, como dados de biometria ou comportamento únicos.

A autenticação de dois fatores (2FA) requer dos usuários apenas dois métodos de autenticação, enquanto a MFA requer pelo menos dois ou mais métodos de autenticação. É importante ressaltar que quantos mais métodos forem incorporados ao processo, maior o atrito (esforço necessário para autenticar a conta) para o usuário.

A figura na página a seguir apresenta exemplos de autenticação 2FA e MFA.



Como aplicar o MFA

Quando se trata de métodos de MFA existem diversas opções disponíveis para sua implementação. No entanto, é necessário compreender que não existe uma abordagem do tipo “solução única para todos os casos”. Em vez disso, a equipe de segurança da informação deve selecionar as alternativas que estejam mais alinhadas com seus casos de uso e representem a experiência de menor atrito para os usuários para garantir uma ampla adoção. As opções de MFA mais comuns incluem:

Perguntas de segurança: Uma ou mais podem ser usadas como forma mais simples de autenticação, usando algo que o usuário conhece.

a preocupação com a qualidade e a utilização de senhas - em torno de 19% dos usuários usam senhas facilmente adivinháveis ou compartilham senhas entre diferentes contas. Evite este comportamento e use multifator de autenticação sempre que possível; e

Tokens OATH TOTP (*Open Authentication Time-Based One Time Password*): padrão aberto que especifica como os códigos de senha única (OTP) são gerados. OATH TOTP pode ser implementado usando *software* ou *hardware* para gerar os códigos. Para autenticar usando TOTP (senha única baseada em tempo), o usuário insere um código de 6 a 8 dígitos que muda a cada 30 segundos. O código é gerado usando HMAC (segredo compartilhado, *timestamp*), em que o *timestamp* muda a cada 30 segundos.

Notificações *push* móveis: As notificações *push* móveis para um aplicativo de autenticação móvel para dispositivos *iOS* e *Android* permitem um simples deslizar após desbloquear o *smartphone* para verificar a autenticação.

Chaves de autenticação em *hardware* (*Hardware* OATH) - normalmente vêm na forma de um *smartcard* ou USB *eToken* usado como senha única segura que pode ser usada para autenticação multifator (MFA). É uma arquitetura de referência aberta para implementar autenticação forte. O algoritmo de criptografia é um padrão de código aberto e, como tal, está amplamente disponível.

Cabe ressaltar que o uso da 2FA ainda é extremamente irregular, com apenas 32,4% dos entrevistados utilizando esse método para todos os aplicativos. 37,9% dos entrevistados utilizavam a 2FA para apenas alguns aplicativos. Infelizmente, muitas pessoas ainda não usam MFA consistentemente pois consideram as etapas de segurança adicional como uma inconveniência que elas evitarão se possível.

Vulnerabilidades relacionadas à MFA

Cabe ressaltar que o uso da 2FA ainda é extremamente irregular, com apenas 32,4% dos entrevistados utilizando esse método para todos os aplicativos. 37,9% dos entrevistados utilizavam a 2FA para apenas alguns aplicativos. Infelizmente, muitas pessoas ainda não usam MFA consistentemente pois consideram as etapas de segurança adicional como uma inconveniência que elas evitarão se possível.

Infelizmente, a adoção de alguns dos métodos de MFA provaram não ser suficientes. Ataques e incidentes recentes mostram que os profissionais de segurança ainda têm um longo caminho a percorrer de forma a garantir implementações de autenticação 2FA e MFA mais robustas.

Existem diversas maneiras de quebrar a segurança da MFA, dentre elas:

- Ataques *man-in-the-middle* baseados em SMS;
- Ataques por *Push*;
- Desvio do fluxo de autenticação MFA; e
- Ataques *pass-the-cookie*.

a) Ataques *man-in-the-middle* baseados em SMS.

O maior problema com o MFA tem a ver com sua implementação mais comum: usar senhas descartáveis (OTP) SMS. Já existe farta documentação comprovando que os OTPs transmitidos por SMS são vulneráveis à interceptação (por exemplo, troca de SIM ou golpes de portabilidade de número de celular). Inclusive, por esse motivo, o *National Institute of Standards and Technologie* (NIST) em sua publicação especial 800-63 *Guidelines* recomendou restringir o uso de OTP via SMS e eliminar completamente a opção de envio de OTP por *e-mail*.

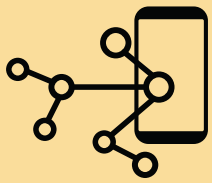
A fraqueza tem a ver com dois fatores:

- a facilidade com que os *hackers* podem comprometer os *smartphones* dos usuários e atribuir o número de telefone temporariamente a um telefone sob seu controle; e
- a transmissão de mensagens SMS em texto livre (as mensagens SMS não são criptografadas).

Existem várias maneiras de realizar esse ataque. As mais comuns são:

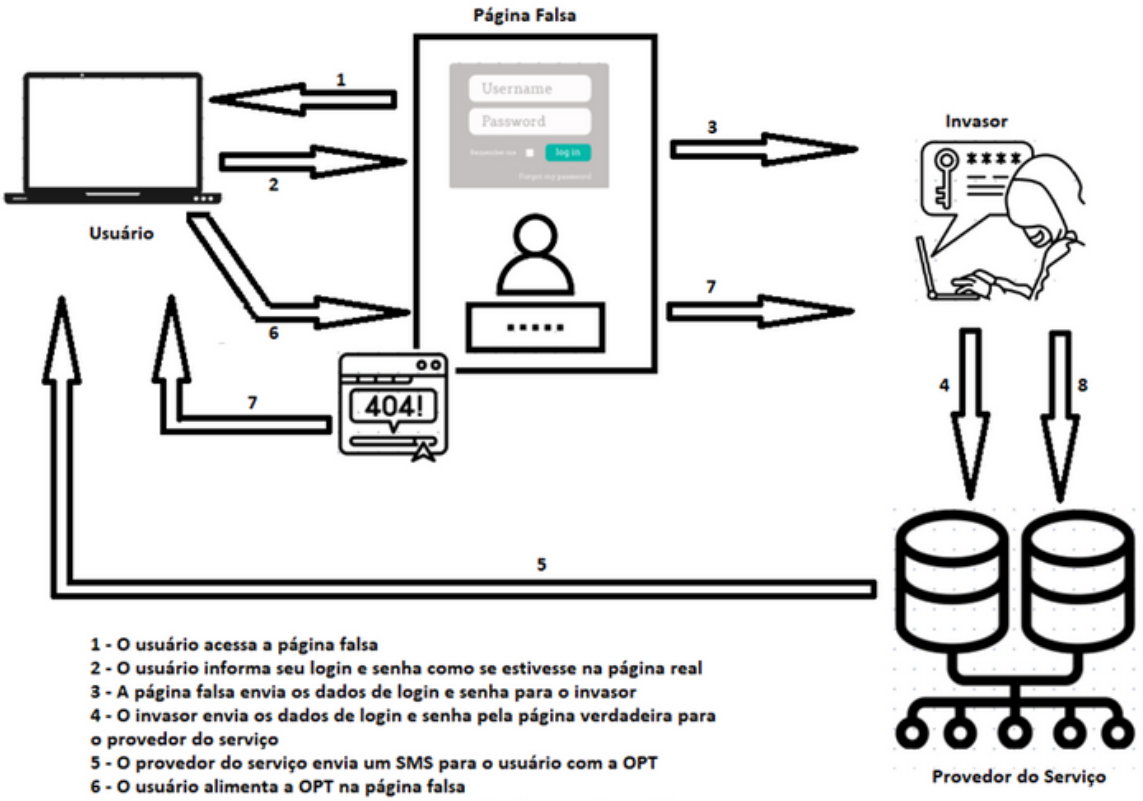
- **SIM *Swapping***, onde os invasores enganam (usando engenharia social) ou subornam funcionários de serviços de telecomunicações para portar o número de telefone de um alvo para seu próprio cartão SIM. Esse tipo de ataque é rapidamente percebido pois a vítima perde totalmente o serviço do celular;

- **Ataques SS7**, que são ataques cibernéticos que exploram vulnerabilidades no protocolo SS7 de forma a comprometer e interceptar comunicações de voz e SMS na rede celular. Tudo o que um invasor precisa para lançar um ataque SS7 com sucesso é um computador executando *Linux* e o SS7 SDK – ambos gratuitos para *download* da *Internet*. Uma vez conectado a uma rede SS7, o invasor pode atingir os assinantes na rede enquanto engana a rede fazendo-a pensar que o dispositivo invasor é na verdade um nó da rede.
  As falhas e vulnerabilidades inerentes ao protocolo SS7 estão fora da jurisdição de empresas e consumidores. Sendo assim, as vulnerabilidades do SS7 não podem ser simplesmente removidas ou corrigidas.



- **Burlar os procedimentos de um serviço de SMS comercial**, que permite às empresas enviar lembretes, alertas, confirmações e campanhas de *marketing* por SMS, de forma a redirecionar as mensagens de um alvo para o invasor. Esse vetor de ataque é extremamente negligenciado e utiliza principalmente as lacunas na regulamentação dos serviços de SMS comerciais, com um invasor muitas vezes sendo capaz de atingir seus alvos apenas informando – falsamente - que tem o consentimento do alvo, uma vez que o provedor do serviço nunca confirma o consentimento com o usuário alvo.

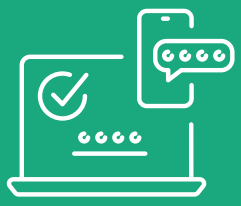
- **Uso de páginas falsas que imitam serviços reais para obter o código 2FA via SMS.**



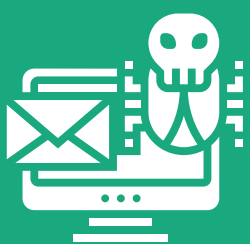
1 - O usuário acessa a página falsa
2 - O usuário informa seu login e senha como se estivesse na página real
3 - A página falsa envia os dados de login e senha para o invasor
4 - O invasor envia os dados de login e senha pela página verdadeira para o provedor do serviço
5 - O provedor do serviço envia um SMS para o usuário com a OPT
6 - O usuário alimenta a OPT na página falsa
7 - A página falsa envia a OPT para o invasor. Geralmente, ela também envia ao usuário uma mensagem de erro, a fim de evitar suspeita.
8 - De posse da OPT, o invasor completa o processo de 2FA e agora tem o acesso completo à conta do usuário alvo.

Esse é um processo mais elaborado, que implica em levar o usuário primeiro a entrar na página falsa e após o processo inicial de autenticação (*login* com conta e senha), redirecionar esses dados para o serviço real para que ele envie o código 2FA via SMS para o alvo. Ao mesmo tempo, o invasor apresenta, na página falsa que o usuário está acessando a solicitação do código 2FA enviado pelo serviço real. Quando o alvo informa o código 2FA na página falsa, o invasor passa a ter todos os componentes necessários para continuar seu ataque.

b) Ataques por *Push*



A autenticação por *push* é uma das formas de autenticação mais fáceis de usar. Muitas organizações implementam a MFA com a autenticação por *push* para proteger seus usuários. O processo é simples: após o envio de *login* e senha, o usuário recebe uma notificação em um dispositivo móvel cadastrado para aprovar o acesso, devendo tocar em "aprovar" ou "negar" (ou "sim" ou "não" ou alguma variação desses termos).



Os ataques por *push* (também chamados de ataques de notificação por *push*, ataques de fadiga por *push* e bombardeio de *prompt* de MFA) são usados por invasores como uma forma de passar pela MFA de autenticação por *push*. O invasor geralmente já possui um nome de usuário e senha válidos. Afinal, com mais de 15 bilhões de senhas roubadas disponíveis na *dark web*, isso é trivial. O invasor envia *spams* às suas possíveis vítimas com notificações para autenticação até que uma delas aprove a solicitação. Quando implantado em grande escala usando ferramentas de ataque automatizadas, mesmo uma taxa de sucesso de 3% é significativa.

O método é considerado extremamente vantajoso pelos invasores pois eles atuam sobre o seguinte cenário: O que acontece quando um usuário está ocupado, imerso em seu trabalho, e recebe uma notificação em seu dispositivo móvel para aprovar?

- O usuário sempre lê a notificação?
- Qual é a probabilidade de um usuário aprovar casualmente uma notificação por *Push* apenas por hábito ou para continuar suas tarefas do dia?
- Um usuário menos experiente tocaria em "Aprovar" em seu aplicativo móvel, mesmo que fosse uma notificação por *Push* falsa?

Os ataques por *Push* utilizam os seguintes fatores de vulnerabilidade:

- Conhecimento – os ataques por *Push* se aproveitam principalmente da falta de conhecimento sobre o assunto por parte dos usuários. A maioria das organizações têm concentrado seus esforços e investimentos em educação de segurança para proteger os seus usuários e funcionários de serem vítimas de ataques mais tradicionais, como o *phishing*. Ainda vai demorar um tempo que o ataque por *Push* faça parte do vocabulário diário dos usuários.

- Familiaridade - as aprovações baseadas em *Push* geralmente são introduzidas por uma organização junto com um aplicativo MFA, como uma forma de aumentar a segurança do serviço. Isso leva o usuário a associar a ação de aprovar uma solicitação a um recurso de segurança. Diante disso, é compreensível que a grande maioria das pessoas não suspeitem dos riscos vinculados a essa funcionalidade.

- Sobrecarga cognitiva – Em função de grande quantidade de alertas relativos a *e-mails*, SMS, eventos da agenda, mensagens de W*hatsapp*, etc., os dispositivos ficam sobrecarregados de notificações. Simplesmente há muita informação para processar – e os invasores tiram proveito dessa sobrecarga pois entendem que vários usuários que recebem dezenas ou mesmo centenas de notificações por dia provavelmente não pensarão muito sobre elas. A probabilidade de uma única aprovação de *login* fraudulenta ser ignorada ou aprovada por acidente é baixa, mas em escala torna-se um vetor de ataque muito promissor.

- Ataques *man-in-the-middle* – assim como ocorre no ataque ao SMS, o invasor também pode enviar as credenciais de diversos usuários para o serviço desejado e apenas esperar que um usuário aprove a solicitação de *login*.

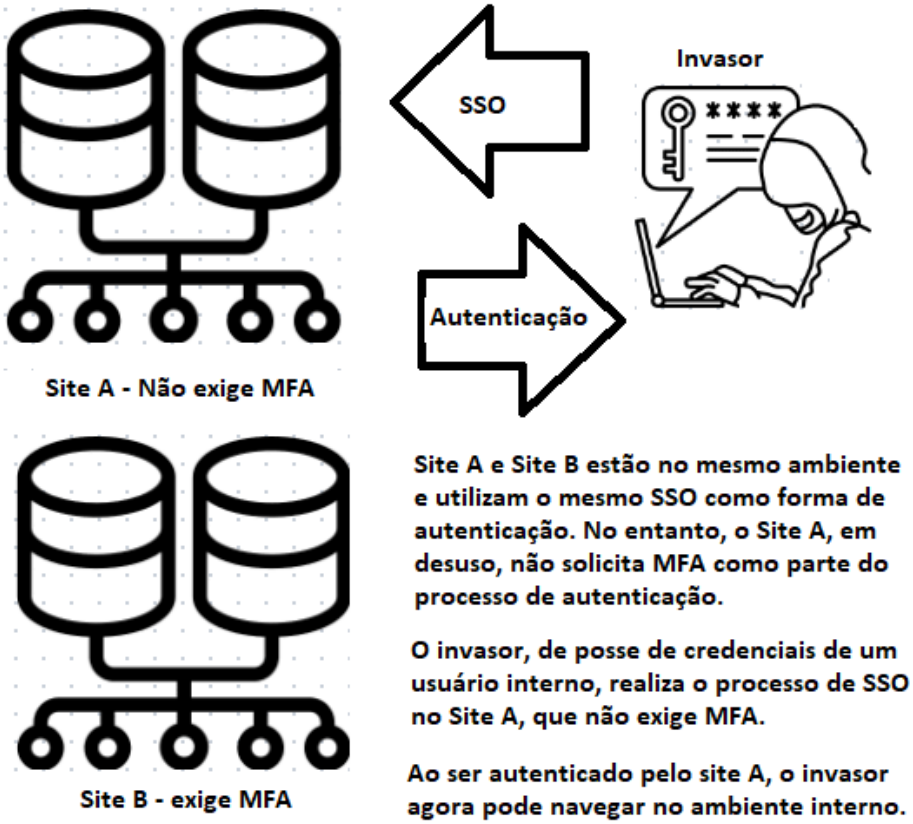
O maior problema reside no fato de que muitos usuários estão propensos a aprovar uma notificação por PUSH sem sequer ler seu conteúdo, pois essas notificações tornaram-se tão numerosas que as pessoas muitas vezes as aprovam apressadamente - sem saber ou entender as repercussões que isso pode ter.

c) Desvio do Fluxo de Autenticação MFA

A implementação da solução de autenticação MFA pode estar comprometida de forma a permitir a um invasor simplesmente realizar um desvio do fluxo de autenticação e obter acesso aos recursos desejados.

Uma das formas de realizar esse ataque é explorar uma má implementação do sistema de autenticação.

Um cenário comum consiste em encontrar sistemas externos não protegidos por MFA como, por exemplo, um ambiente que utilize o mesmo sistema SSO (*Single-Sign On*) no qual um dos sites exija MFA e o outro não. Numa situação como essa, um invasor poderia simplesmente *logar* no site que não exige a MFA como uma forma de acessar a conta de um usuário apenas desviando da MFA.



Por exemplo, o perímetro externo de uma organização pode impor MFA no *Microsoft365* e em sua VPN SSL. No entanto, um antigo portal Citrix não usado mais pelos funcionários foi esquecido durante a implantação da MFA. Este sistema seria um alvo de escolha para um invasor com credenciais comprometidas para conseguir um ponto de apoio na rede interna.

A existência de erros na lógica na aplicação é outra vulnerabilidade que permite o desvio do fluxo de autenticação MFA .

Às vezes, os invasores podem derrotar a MFA simplesmente explorando os erros de lógica do aplicativo no processo de autenticação. Um erro lógico comum que compromete o MFA é a a existência de uma etapa de autenticação que possa ser ignorada, o que poderia permitir aos usuários pular uma etapa no processo de autenticação.

Tomemos como exemplo a seguinte situação de MFA em três etapas:

Passo 1 (verificação da Senha) -> Passo 2 (código em *hardware*) -> Passo 3 (pergunta de segurança)

Sendo que a aplicação deveria funcionar da seguinte forma:

1. Pagina_de_acesso/*login* (solicita a senha do usuário -> Passo 1)
2. Caso as credenciais estejam corretas, envia a página MFA_HWC
3. Pagina_de_acesso/MFA_HWC (solicita o envio do código de *hardware* armazenado pelo usuário - > Passo 2)
4. Caso o código de *hardware* seja válido, envia a pergunta de segurança
5. Pagina_de_acesso/MFA_perguntadeseguranca (solicita o envio da resposta à pergunta de segurança -> Passo 3)
6. Caso a pergunta de segurança seja respondida corretamente, autoriza a solicitação de *login*

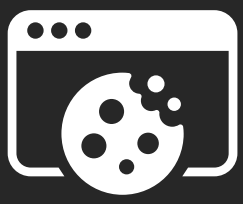
Aparentemente, o processo parece estar correto. No entanto, veja que o passo 6 "autoriza a solicitação de *login*" CASO a pergunta de segurança seja respondida corretamente. Ou seja, a lógica adotada foi a de que o usuário obrigatoriamente realizará todos os passos a fim de obter a autorização de *login*, desconsiderando a possibilidade de que um ator seja capaz de pular o passo 2 do processo de MFA.

Na prática, com essa lógica adotada, seria possível a um invasor, após informar o *login* e senha do usuário (que, como já foi visto, é trivial de ser obtido), enviar um *request* diretamente para Pagina_de_acesso/MFA_perguntadeseguranca com a resposta correta (pois é bem mais fácil descobrir a resposta de uma pergunta de segurança do que falsificar um código de *hardware* de posse do usuário). Nesse caso, o invasor evitaria o redirecionamento MFA_HWC e teria sua solicitação de *login* autorizada.

A correção desse erro de lógica seria simples, pois bastaria alterar o item 6. para:

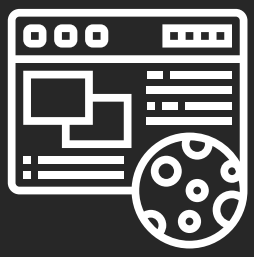
6. Caso MFA_HWC E MFA_pergunta_de_seguranca estejam corretos, autoriza a solicitação de *login*.

d) Ataques *pass-the-cookie*



Os *cookies* do navegador permitem que os aplicativos da *Web* armazenem informações de autenticação do usuário, para que um usuário possa permanecer conectado em vez de fornecer seu nome de usuário e senha sempre que navegar para uma nova página em um *site*.

Se o MFA estiver ativado, o usuário deverá fornecer prova adicional de sua identidade, como aceitar uma notificação por *PUSH* em seu dispositivo móvel. Depois que o usuário passa pela MFA, um cookie do navegador é criado e armazenado para sua sessão da *web*.



Embora os *cookies* simplifiquem a experiência do usuário, eles carregam uma vulnerabilidade óbvia: se um invasor conseguir extrair os *cookies* corretos do navegador, ele poderá se autenticar como se fosse o usuário em uma sessão totalmente separada do navegador da *Web* em outro sistema, ou seja, o invasor pode usar um *cookie* comprometido para ignorar a autenticação via MFA.

Esse tipo de ataque geralmente é possível quando um servidor da *web* não sinaliza *cookies* de sessão como seguros. Se os usuários não enviarem *cookies* de volta ao servidor por HTTPS, os invasores podem roubar o *cookie* e sequestrar a sessão, ignorando o MFA.

Outra forma de extrair os cookies de um usuário é utilizar o *Mimikatz*. O *Mimikatz* tornou-se a ferramenta padrão para extrair senhas e *hashes* da memória, realizar ataques *pass-the-hash* e criar persistência de domínio.

Por exemplo, num computador com sistema operacional *Windows* e utilizando o *Google Chrome*, os *cookies* são armazenados no seguinte local:

%localappdata%GoogleChromeUser DataDefaultCookies

Os *cookies* de um determinado usuário são criptografados usando chaves vinculadas a esse usuário por meio da API de proteção de dados da Microsoft (DPAPI). Para acessar o banco de dados de *cookies* e descriptografar os *cookies*, um invasor poderia utilizar os seguintes comandos do *Mimikatz*:

dpapi::chrome /in:"%localappdata%GoogleChromeUser DataDefaultCookies" /unprotect

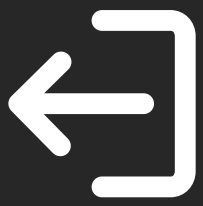
OU

mimikatz.exe privilege::debug log "dpapi::chrome /in:%localappdata%googlechromeUSERDA~ 1defaultcookies /unprotect" exit

Ele obteria como resultado os cookies do browser

```
COMMANDO 4/9/2020 3:24:54 PM
PS C:\Tools\Mimikatz\x64 > mimikatz.exe privilege::debug log "dpapi::chrome /in:%localappdata%\google\chrome\USERDA~1\de
fault\cookies /unprotect" exit

  .#####.   mimikatz 2.2.0 (x64) #18362 Mar  8 2020 13:32:41
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # log
Using 'mimikatz.log' for logfile : OK

mimikatz(commandline) # dpapi::chrome /in:%localappdata%\google\chrome\USERDA~1\default\cookies /unprotect
> Encrypted Key found in local state file
> Encrypted Key seems to be protected by DPAPI
 * using CryptUnprotectData API
> AES Key is: 49fddd81b2271d0967c01718ffcae71b21a9b5898a

Host  : .google.com ( / )
Name  : NID
Dates : 4/6/2020 10:32:48 PM -> 10/6/2020 10:32:48 PM
 * using BCrypt with AES-256-GCM
```

A maneira mais fácil de mitigar a vulnerabilidade MFA *pass-the-cookie* é com melhor gerenciamento de *cookies* e melhor treinamento do usuário.



Especificamente, os *cookies* devem ser definidos com uma vida útil curta e devem ser para uma única sessão, portanto, quando o navegador é fechado, o *cookie* é anulado. Os usuários devem ser treinados para fazer *logoff* do aplicativo da *web* e fechar o navegador após terminarem de usar o aplicativo da *web*. Muitos usuários nunca fazem *logoff* ou fecham um navegador, e isso aumenta o risco.

Na prática, não há uma maneira única de corrigir a vulnerabilidade *pass-the-cookie*, a menos que se force o usuário a se autenticar com mais frequência para diferentes funcionalidades de aplicativos da *web*. Isso, infelizmente, tem um impacto significativo na experiência do usuário.

Atualmente, muitas organizações já implementam soluções mitigadoras, o que significa que esses ataques não são tão bem-sucedidos quanto costumavam ser alguns anos atrás. Essas mitigações incluem apenas permitir o acesso à infraestrutura de nuvem corporativa a partir de endereços IP conhecidos, idealmente por meio de um *endpoint* corporativo de VPN (rede privada virtual) com MFA forte separado. Além disso, os cookies de sessão fornecidos tendem a ser limitados no tempo, portanto, são úteis apenas por um curto período.

Uso de Biometria como Fator de autenticação

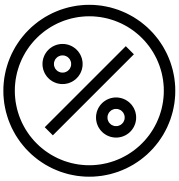
Soluções biométricas são consideradas uma forma muito seguro de autenticação. Além disso, são soluções com baixo custo, fáceis de utilizar e não-intrusivas.

A força da autenticação de qualquer modalidade biométrica é medida em termos da taxa de aceitação falsa (*false acceptance rate* – FAR), ou seja, um erro que permite o acesso indevido a um invasor.

A FAR é expressa como uma porcentagem de tentativas nas quais ocorreu um falso positivo, ou seja, se o FAR for 0,001%, isso significa que 1 em cada 100.000 tentativas resultará num falso positivo.

Em contrapartida, as dificuldades na utilização de uma modalidade biométrica são medidas em termos da taxa de rejeições falsas (*false rejection rate* – FRR), ou seja, um erro que impede o acesso a um usuário legítimo.

A FRR é expressa como a porcentagem de tentativas que resultaram num falso negativo. Por exemplo, se o FRR for 0,02%, um em cada 5.000 usuários legítimos não será reconhecido ao tentar obter acesso ao recurso desejado.

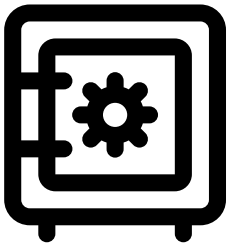


A FAR e FRR têm um único ponto de interseção. A coincidência dos indicadores percentuais neste ponto indica a igualdade das taxas. Tal ponto é chamado de taxa de erro igual (*Equal Error Rate* - EER). Idealmente, o indicador EER deve ser zero, o que significa que FAR e FRR também são iguais a zero. Na prática, isso é inatingível.

FAR e FRR estão em um estado de equilíbrio. Ao diminuir o FAR, o nível FRR aumentará e vice-versa. A FAR é responsável pela segurança, enquanto a FRR está relacionada à conveniência para o usuário final.

Em última análise, é necessário decidir o que é mais importante: usabilidade ou segurança.

De maneira geral, estabelecimentos de alta segurança (cofres de banco e instalações militares, por exemplo), onde a preocupação contra invasões é grande, devem operar com uma FAR baixa, sendo preferível uma taxa de rejeição maior que de aceitação, pois as consequências do acesso não-autorizado podem ser graves.



Em contrapartida, em aplicações forenses, onde a necessidade de identificar um criminoso supera os inconvenientes de examinar um grande número de suspeitos, a FRR deve ser relativamente baixa.

Aplicações civis, de uso geral, tendem a balancear a FAR e FRR. Estas aplicações, usualmente, operam com uma EER onde a FAR é igual, ou muito próxima, da FRR. É importante salientar que o mesmo sistema biométrico poderia ser utilizado em qualquer um desses casos, porém com escolhas de diferentes valores do limiar.

As características do leitor biométrico utilizado podem afetar os níveis de FRR. Após conectar o leitor e instalar o *software*, é criado um modelo de cadastro para cada indivíduo, a partir do qual funciona o sistema biométrico. É desejável que a qualidade desse modelo seja alta o suficiente para reduzir os problemas de FRR associados à correspondência de varreduras biométricas com modelos.

1

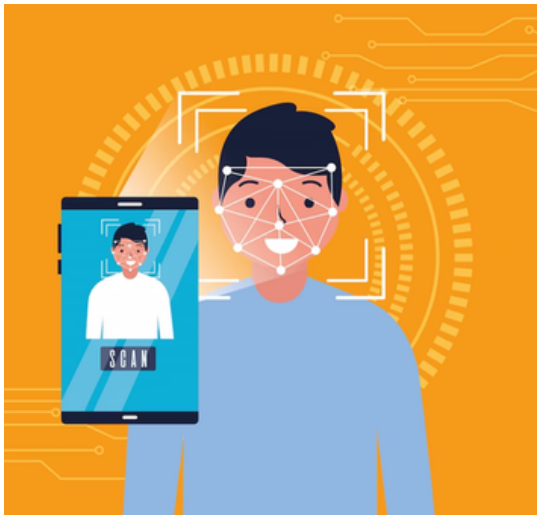
Uso de Impressão Digital como Fator de autenticação

Resultados apresentados em trabalhos sobre o tema mostram que as impressões digitais são boas o suficiente para proteger a privacidade da pessoa comum. De maneira geral, qualquer técnica de clonagem de impressão digital a ser aplicada em bons dispositivos biométricos é difícil, trabalhosa e relativamente onerosa, tornando a autenticação por impressão digital um método válido. No entanto, uma pessoa com um perfil de alto risco e que provavelmente será alvo de um agente bem financiado e motivado não deve usar apenas a autenticação de impressão digital.

2

Uso de Reconhecimento Facial como Fator de autenticação

A tecnologia de reconhecimento facial usa um banco de dados de fotos para identificar pessoas em fotos e vídeos de segurança. Ela usa biometria para mapear recursos faciais e ajudar a verificar a identidade por meio dos principais recursos do rosto. A característica mais importante é a geometria de um rosto, como a distância entre os olhos de uma pessoa e a distância da testa ao queixo. Isso então cria o que é chamado de "assinatura facial". É uma fórmula matemática que é então comparada a um banco de dados de rostos conhecidos.O reconhecimento facial também apresenta desafios. Como a face de uma pessoa geralmente é tratada pelos dispositivos biométricos como um dado estático, os invasores têm utilizado fotos de diferentes fontes, inclusive das mídias sociais, para tentar burlar os sistemas biométricos de reconhecimento facial.



3

Uso de Reconhecimento de Íris como Fator de autenticação

Dentre todos os métodos biométricos, os sistemas baseados no reconhecimento de íris vêm ganhando destaque em virtude de serem considerados como uma das modalidades biométricas mais precisas. As altas taxas de reconhecimento obtidas devem-se, em parte, à complexidade fisiológica de cada íris, que resulta na formação de padrões aleatórios de textura, sendo estatisticamente exclusivos e, portanto, adequados para um sistema biométrico de identificação pessoal. Os dados da biometria da íris são armazenados como códigos de íris. Geralmente, um código de íris contém cerca de 5.000 informações diferentes. Uma das etapas mais críticas de um sistema de reconhecimento de íris é a etapa de segmentação, na qual a região da íris é localizada e extraída a partir de uma imagem do olho previamente coletada, para que os modelos biométricos posteriormente gerados contenham apenas informações de íris.

Na prática, a complexidade da segmentação é proporcional à qualidade e característica da imagem capturada, tendo em vista que este procedimento é dificultado nos casos em que as imagens obtidas durante a etapa de aquisição estiverem corrompidas por ruídos.

Os ruídos mais comuns encontrados são:

- Obstrução da pupila por pálpebras: as pálpebras são uma das maiores fontes de ruído nas imagens porque sobrepõem-se à grandes porções de pupila nos extremos superiores e inferiores.
- Obstrução da pupila por cílios: este tipo de ruído é bastante comum e ocorre principalmente a partir dos cílios das pálperas superiores.
- Obstrução da pupila por reflexões especulares: causado devido ao esquema de iluminação utilizado durante a coleta da imagem, este tipo de ruído geralmente se apresenta como os pontos de intensidade mais elevada em uma imagem e, frequentemente, interferem na identificação das bordas da região da pupila e da íris.

As técnicas de segmentação de pupila são baseadas na detecção de círculos e, consequentemente, são bastante afetadas por estes ruídos, principalmente pelo ruído causado pelas pálpebras, o que pode aumentar significativamente o FRR.

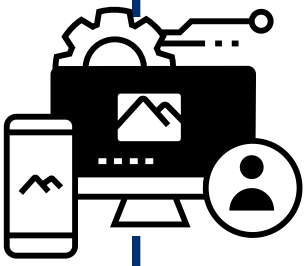
Melhores práticas para uso de MFA

Escolher um fornecedor de MFA confiável

Uma das decisões mais importantes ao implementar a MFA para usuários é escolher o fornecedor certo. Os seguintes aspectos devem ser observados na seleção do fornecedor:

- A forma como é verificada a aderência à conformidade integrada à solução de MFA;
- Capacidade de fornecer suporte para vetores de ameaças em evolução;
- Capacidade de dimensionar a solução de MFA de forma eficaz de acordo com as necessidades da organização;
- O grau de segurança e confiabilidade da solução de MFA;
- O nível de atrito da solução de MFA; e
- Facilidade de implementação e implantação da solução MFA na organização.

Focar na facilidade de uso da solução de MFA



Geralmente, a escolha de uma solução de MFA é feita a partir da avaliação das necessidades da organização, considerando o tipo de dados que precisam ser protegidos e a complexidade dos requisitos de segurança. No entanto, é imperativo considerar o nível de atrito exigido para os usuários.

Se a solução escolhida for muito complexa ou difícil de utilizar, os usuários podem:

- Sofre de fadiga de MFA, ou seja, serem sobrecarregados com tantas notificações que acabem se descuidando e aprovando uma solicitação indevida;
- Tentar contornar a solução de MFA.

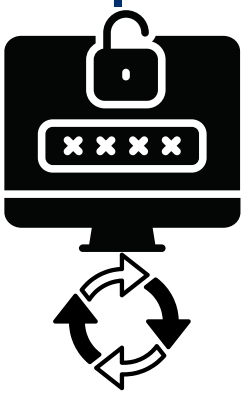
A experiência do usuário é fundamental para o sucesso de uma implantação bem sucedida de MFA, portanto, a conveniência do usuário deve permanecer em primeiro plano.

Oferecer uma variedade de fatores de autenticação

Uma forma de garantir a conveniência de uso da MFA para os usuários é escolher uma solução de MFA que ofereça uma variedade de métodos de autenticação disponíveis para os usuários escolherem. Isso pode incluir uma combinação de biometria, como impressão digital, varreduras de retina e reconhecimento facial, ou outras opções, como *tokens* de *hardware*, SMS/mensagens de texto, verificação de chamada/*e-mail*, perguntas de segurança, *tokens* de *software*.

Além da conveniência de uso, a existência de diferentes tipos de usuários em uma organização torna necessário ter a disposição várias opções de fatores de autenticação.

Por exemplo, dependendo do grau de segurança de uma organização, seus usuários internos podem ser impedidos de utilizar os dispositivos móveis enquanto estiverem no ambiente de trabalho, o que impediria uma solução que se baseasse em autenticação por *Push* ou por SMS. Da mesma forma, usuários que estejam em constante deslocamento sentiriam maior dificuldade em usar um *link* de *e-mail* como uma forma de autenticação ao invés de uma notificação por *Push* ou por SMS.



Usar uma variedade de fatores para MFA também ajuda os usuários a configurar mais de um fator e depois usá-lo conforme sua conveniência.

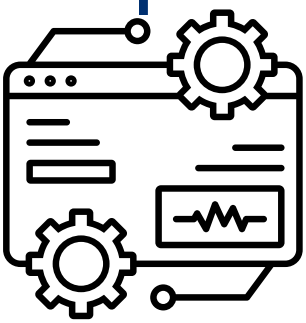
É importante ressaltar que o meio de recuperação de senha e o meio de autenticação de segundo fator não sejam os mesmos.

Por exemplo, se uma organização oferecer recuperação de senha por meio de um *link* de *e-mail*, ela deve certificar-se de não utilizar o *link* de *e-mail* como autenticação de segundo fator pois ter a mesma fonte para recuperação de senha e MFA reduz a segurança para apenas uma fonte - conta de *e-mail* neste caso.

Selecionar soluções de fácil implantação e gerenciamento

Uma das formas de tornar a prática de MFA sustentável numa organização é garantir que o processo de implantação e o gerenciamento da solução de MFA será realizado com facilidade pela equipe de TI.

Idealmente, deve-se procurar soluções que permitam implantar a solução de MFA facilmente para todos os usuários, sem a necessidade de nenhum *hardware* ou *software* adicional.

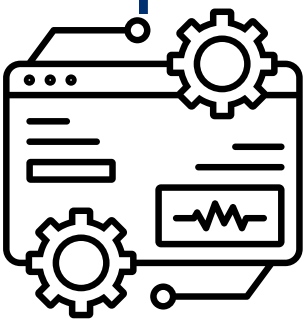


Além disso, deve-se escolher uma solução MFA que se adapte bem à infraestrutura existente. Para isso, a solução deve observar os seguintes fatores:

- capaz de trabalhar com todos os sistemas operacionais utilizados na organização
- permitir sua integração com o sistema de autenticação existentes, como o *Active Directory* ou outro tipo de sistema LDAP em uso. Caso ela não permita essa integração, utilizando um sistema de diretórios próprios, é necessário considerar as dificuldades que podem surgir em sua administração; e
- fornecer mecanismos que permitam sua distribuição de forma centralizada, sem a necessidade de sua instalação, de forma individual, pela organização.

Por fim, recomenda-se que a solução MFA deva ter um painel unificado para que os administradores avaliem rapidamente as consultas dos usuários e possam responder a problemas, quando necessário.

Implementar a solução de MFA em toda a organização



A solução de MFA precisa ser escalável para que possa ser:

- implantada em toda a organização; e
- capaz de crescer junto com a organização.

Não se deve limitar a autenticação MFA a funções de usuário específicas, ou seja, todos os usuários devem ser obrigados a usar autenticação MFA para qualquer acesso à conta em toda a organização, independentemente da confidencialidade das informações. Isso garante que nenhuma conta de usuário fique desprotegida.

Implantar uma solução de MFA apenas para silos ou grupos específicos é um exercício de futilidade e deve-se tomar os devidos cuidados para garantir que todos os pontos de acesso sejam cobertos pela MFA. Isso também inclui todas as cargas de trabalho na nuvem.

As práticas de segurança precisam ser consistentes em toda a organização, com cuidado especial dedicado a MFA em relação ao acesso remoto por seus usuários. Idealmente, a implantação da solução MFA deve abranger todos os usuários finais (incluindo usuários privilegiados), aplicativos na nuvem e locais, VPN, *logins* de servidor e elevação de privilégios.

Proteger todos os tipos de usuários é o objetivo final do processo. A fase de implantação pode abranger um tipo de cada vez e gradualmente abranger todos os tipos de usuários.

Utilizar uma solução de MFA adaptável

Em alguns cenários, pedir constantemente aos usuários que concluam a MFA para autenticação pode ser uma experiência frustrante. Nesses casos, a adoção de autenticação adaptável ou progressiva é uma abordagem melhor.

Uma solução MFA adaptável usa informações contextuais para determinar se deve solicitar outro fator para autenticação do usuário ou não.

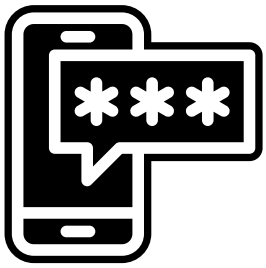
Esses contextos podem ser localização, IP, rede, dispositivo, comportamento ou qualquer coisa completamente dependente de requisitos definidos pela organização. Essa abordagem também é útil para proteger contas contra ataques de força bruta. Por exemplo, o contexto pode ser “solicitar outro fator para concluir a autenticação se a senha errada for digitada 3 vezes consecutivas”.

Educar os usuários em relação a MFA

Parece um ponto simples, mas educar os usuários é uma das práticas recomendadas mais importantes para a devida adoção da MFA. A maioria dos pesquisadores acredita que o elo mais fraco na cadeia de segurança é o usuário. Portanto, nenhuma quantidade de parâmetros pode garantir uma melhor segurança se os usuários não a estiverem usando de maneira eficaz.

É crucial começar a educar adequadamente os usuários sobre a importância da MFA e sobre como usá-la corretamente. Em especial, os usuários devem compreender os seguintes aspectos:

- As necessidades e vantagens para o usuário em adotar uma MFA; e
- O objetivo final da adoção de uma MFA para a organização.

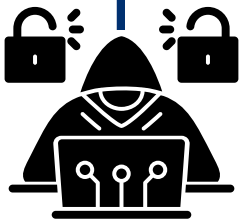


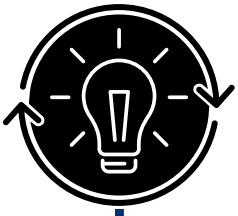
Combinar a MFA com o *Single-Sign On* (SSO)

A autenticação SSO oferece uma ótima experiência do usuário, e a combinação da MFA com SSO pode oferecer uma experiência de usuário mais tranquila e fortalecer a segurança.
Além disso, dessa forma, os usuários não precisam inserir uma senha na primeira etapa da autenticação, pois o SSO usa uma conta de usuário existente para isso. Ao mesmo tempo, a segunda etapa da autenticação permanece a mesma do caso de autenticação por senha, ou seja, um OTP, *link* de *e-mail*, *token*, biometria, etc.

Estabelecer um fator de resistência

Embora a MFA forneça segurança adicional, ela também é vulnerável a ataques, especialmente se não for implementado corretamente.
Como prática recomendada geral de MFA, as organizações precisam garantir que sua solução MFA seja configurada com segurança e que os usuários saibam como usá-la com eficiência.
Além disso, as organizações devem implantar diferentes fatores de autenticação com base em funções. Contas privilegiadas devem sempre utilizar fatores de alta resistência a ataques (isso geralmente cria um maior nível de atrito). Fatores considerados bons o suficiente, mas que gerem menor nível de atrito, podem ser implantados para funções de usuário com menos privilégios.

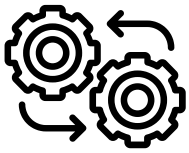




Reavaliar a MFA periodicamente

As ameaças de segurança estão sempre evoluindo. Por este motivo, as organizações devem reavaliar periodicamente a MFA para garantir que a solução implementada ainda atenda às necessidades dos usuários e das organizações e, ao mesmo tempo, também atenda aos requisitos de segurança refinados.

Considerações finais



A maioria das organizações é muito hábil e rápida em se adaptar a novas tecnologias para obter melhores resultados de negócios ou produtividade, mas isso raramente é o caso quando se trata de melhorar sua postura geral de segurança.

Os benefícios do uso de autenticação MFA não estão limitados à área de TI. Embora seja do conhecimento geral que o uso de MFA pode proteger contra acesso não autorizado, violação de dados e ataques cibernéticos baseados em senha, os benefícios do uso da MFA vão muito além da segurança e essas são implicações que devem ser de conhecimento tanto da alta administração da organização bem como de seus usuários, internos e externos.

Dentre os benefícios esperados pelo uso de autenticação MFA temos:

- Maior confiança dos usuários e da cadeia de suprimentos – a segurança está começando a desempenhar um grande papel na forma como uma organização é percebida por outras pessoas no setor e, mais importante, por seus usuários. Isso inclusive pode ser o fator decisivo numa decisão de estabelecimento de acordos entre organizações. Ressaltar o compromisso da organização com a segurança, adotando em conjunto com a MFA um padrão *Zero Trust Security*, por exemplo, tem um alto impacto na percepção dos usuários e potenciais parceiros.
- Redução dos custos operacionais – o bom uso de autenticação MFA pode reduzir sensivelmente os custos operacionais de uma organização. Basta, por exemplo, calcular quanto custa cada vez que uma organização precisa notificar seus usuários sobre atividades suspeitas em suas contas. A autenticação MFA reduz sensivelmente o risco de fraude, exigindo menos esforços de suporte técnico e deixando a equipe de serviço livre para se concentrar em problemas mais técnicos ou de negócios. Embora a implantação da MFA certamente irá exigir um investimento inicial, esse custo se pagará muitas vezes a longo prazo.
- Melhor controle do roubo e fraude de identidade – o roubo de senhas tem se tornado trivial para a maioria dos invasores. A autenticação MFA torna essa atividade muito mais difícil ao exigir dois ou mais métodos de verificação de identidade. Isso leva automaticamente a uma redução significativa no número de fraudes e roubo de identidade que as organizações enfrentam regularmente, graças as medidas de segurança adicionais implantadas e informações que não estão facilmente disponíveis para agentes mal-intencionados.

Vale ressaltar que a Secretaria de Segurança da Informação e Cibernética (SSIC) também recomenda aos usuários das diversas organizações, além das orientações apresentadas nesta OSIC, que:

- promovam, divulguem e incentivem o uso do múltiplo fator de autenticação (MFA); e
- informem imediatamente à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) de sua instituição a ocorrência de um incidente cibernético.

Outras Orientações de Segurança da Informação e Cibernética (OSICs) estão disponíveis em https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/osic e propostas de temas, sugestões ou outras contribuições para serem abordadas em futuras OSICs podem ser encaminhadas ao *e-mail* educa.si@presidencia.gov.br.

TLP:CLEAR