O USO DE AUTENTICAÇÃO MULTI-FATOR (MFA) E SUA IMPORTÂNCIA

THE USE OF MULTI-FACTOR AUTHENTICATION (MFA) AND ITS IMPORTANCE

Talita de Oliveira Maia, Faculdade de Tecnologia de Americana (FATEC Americana), talita.maia01@fatec.sp.gov.br
Vitor Furlaneto Alves, Faculdade de Tecnologia de Americana (FATEC Americana), vitor.alves25@fatec.sp.gov.br
Maxwel Vitorino da Silva, Faculdade de Tecnologia de Americana (FATEC Americana), maxwel.silva5@fatec.sp.gov.br

Resumo

No cenário atual, a segurança da informação desempenha um papel crucial, tanto no mundo corporativo quanto na vida cotidiana. Reconhecendo a importância dos dados como ativos valiosos, é essencial explorar todas as camadas de proteção disponíveis no mercado. Nesse contexto, a autenticação multifator (MFA) emerge como uma ferramenta indispensável para proteger contra ameaças de invasão. Embora sua implementação possa causar algum incômodo aos usuários, seus benefícios em termos de segurança são inegáveis. Um exemplo notável é a resistência que o MFA oferece contra ataques de força bruta, tornando-os ineficazes ao exigir autenticação por meio de múltiplos fatores. Idealmente, a utilização de todos os métodos de autenticação multifatorial disponíveis seria a máxima barreira de segurança, mas sua viabilidade depende de fatores como custo e necessidades específicas. Este artigo tem como objetivo apresentar e enfatizar a importância da utilização da autenticação de dois ou mais fatores (MFA), utilizando de pesquisas, coletas e levantamentos de dados a fim de garantir mais segurança para usuários e organizações.

Palavras-chave: Autenticação, segurança, acesso, usuário, invasão

Abstract

In the current scenario, information security plays a crucial role, both in the corporate world and in everyday life. Recognizing the importance of data as valuable assets, it is essential to explore all available layers of protection in the market. In this context, multifactor authentication (MFA) emerges as an indispensable tool to safeguard against invasion threats. Although its implementation may cause some inconvenience to users, its security benefits are undeniable. A notable example is the resistance that MFA offers against brute-force attacks, rendering them ineffective by requiring authentication through multiple factors. Ideally, the utilization of all available multifactor authentication methods would be the ultimate security barrier, but its feasibility depends on factors such as cost and specific needs. This article aims to present and emphasize the importance of using two or more factors authentication (MFA), based on research, data collection, and analysis, in order to provide enhanced security for users and organizations, ensuring the integrity and confidentiality of critical information.

Keywords*: Authentication, security, access, user, invasion*

1. INTRODUÇÃO

Atualmente, ao redor do mundo, é gerado um grande volume de dados ORACLE (2023), trazendo preocupações crescentes em relação à integridade e privacidade desses dados e fazendo com que cada vez mais a Segurança da Informação ganhe destaque e seja um assunto crucial dentro das organizações.

Segundo Martins (2021), a Segurança da Informação (SI) é um conjunto de ações e estratégias que tendem proteger os dados de uma organização. Sendo assim, a SI tem o objetivo de preservar a integridade dos dados de ameaças que podem gerar prejuízos à organização e seus clientes. Dessa forma, são definidas políticas, processos internos e ferramentas a fim de mitigar os riscos e evitar que essas informações sejam expostas de forma indevida.

Diante das recentes discussões sobre privacidade e segurança de dados advindas da aprovação da Lei Geral de Proteção de Dados (LGPD), muitas organizações se atentaram ainda mais para a importância de proteger seus ativos, além das informações de seus clientes, contra possíveis golpes e exposições indevidas. Assim, para se ter sucesso na cibersegurança da organização, faz-se necessário investir cada vez mais em tecnologias que consigam garantir isso.

De acordo com CETAX (2022) a crescente digitalização traz uma enorme quantidade de usuários e dados que trafegam simultaneamente a todo o momento, tanto empresas, que tem a preocupação em assegurar que suas informações e as informações de seus parceiros e clientes estejam seguras, por outro lado, usuários finais também querem manter a confidencialidade de seus dados que essas empresas tratam e armazenam.

CAETANO (2023) cita que hackers ou cibercriminosos são termos utilizados para pessoas que possuem diversos conhecimentos técnicos sobre assuntos que compõem o mundo da tecnologia da informação (T.I). E esses hackers e/ou cibercriminosos, através dos meios de conhecimentos técnicos tem a capacidade de tirar vantagens através de informações.

Das muitas vantagens que um cibercriminoso pode obter ao ter acesso às informações sigilosas a principal delas é a capacidade de chantagear ou até ameaçar a pessoa cujos dados pertencem, geralmente em troca de dinheiro. Ele também pode usar essas informações para fazer empréstimos em bancos ou dívidas no nome do proprietário dos dados.

Essas vantagens podem ser obtidas através da exploração de vulnerabilidades no sistema, e é aí que entra o MFA (do inglês, "*Multi-Factor Authetication*"). Porém, o MFA nem sempre é perfeito, ele também possui algumas vulnerabilidades que podem ser exploradas pelos cibercriminosos para que eles possam obter informações confidenciais.

O MFA é um fator essencial para a política de gerenciamento de acessos e identidades dentro das organizações. Pois segundo FALCÃO (2022) além de evitar roubos de conta e prejuízos financeiros para clientes e organizações, o MFA pode ser entendido como um reforço às políticas de compliance da organização, indicando o comprometimento com a proteção de dados dos usuários, além de fornecer uma camada adicional de proteção, pois os usuários só podem se autenticar depois de fornecer com êxito, dois ou mais elementos de autenticação, evitando assim os possíveis hackers. Nesse contexto, então, justifica-se a relevância desta pesquisa.

O propósito deste artigo é enfatizar a importância da utilização da autenticação de dois ou mais fatores, desta forma, respondendo à questão (problema de pesquisa): "Por que o método de MFA é tão importante e por que as empresas têm adotado?".

2. Revisão bibliográfica

2.1 Autenticação por Multifator

De acordo com MENDONÇA (2022) autenticação por multifator é o uso de dois ou mais fatores para a verificação de autenticidade de um usuário, ou seja, um procedimento de login que utiliza mais de uma etapa de autenticação para garantir a identidade do usuário ao acessar alguma ferramenta ou aplicação.

Conforme VIANA (2022), ao fazer o uso da MFA, se uma senha for comprometida, os cibercriminosos teriam que romper pelo menos mais uma barreira de segurança para conseguir ter acesso à conta e/ou realizar ações específicas, dificultando qualquer tipo de ação criminosa. Logo, trata-se de um procedimento importante para segurança, uma vez que nome de usuário e senha são relativamente fáceis de serem descobertos e frequentemente são utilizados de forma repetida para acessar diferentes contas, aumentando as chances de ataques.

Segundo MENDONÇA (2022), existem algumas práticas que são recomendadas para

as empresas a fim de proteger os recursos digitais e garantir a segurança dos acessos, são algumas:

- a criação de funções diferentes de acesso como os de administradores, gerentes e outros usuários que são menos privilegiados;
- utilização de políticas fortes para criação de senha: solicitar obrigatoriamente que a senha possua caracteres especiais, letras maiúsculas e minúsculas e até números
- e por fim usar diferentes credenciais de segurança como solicitar a alteração de senha com certa frequência, normalmente a cada 90 dias.

De acordo com ARMANI (2019), o funcionamento do MFA vai além da utilização de usuário e senha, pois é feito uma segunda autenticação com envio de um código ou senha para o e-mail ou dispositivo móvel do usuário, a fim de garantir a confiabilidade de que quem está tentando acessar seja o proprietário daquele dispositivo ou aplicação.

VIANA (2022) diz que um dos maiores desafios enfrentados pelas organizações e usuários hoje em dia é o de se proteger contra ameaças digitais de invasão de contas, devido aos grandes problemas e prejuízos que se pode ter com contas invadidas e informações expostas indevidamente.

O MFA exige que os usuários forneçam duas ou mais evidências para obter acesso a ferramenta, podendo diminuir a probabilidade de invasão, essas informações podem ser divididas em três categorias:

- Conhecimento: fatores que os usuários têm conhecimento, como senhas, PIN, respostas para perguntas de segurança.
- Posse: objetos que os usuários têm como crachás, cartões inteligentes, certificados por softwares, tokens etc.
- Inerência: informações únicas de cada pessoa, como impressões digitais, reconhecimento fácil ou de voz.

FALCÃO (2022) afirma que, os benefícios da MFA ainda se alinham com a melhora da postura de cibersegurança da empresa, evitando roubos de dados e contas e consequentes prejuízos financeiros. Assim, as organizações passam a seguir boas práticas de conformidade, aplicando também o compromisso com clientes e colaboradores.

> À medida que as tecnologias de segurança avançaram, o volume de dados a serem protegidos cresceu imensamente. Os dados se movem com os terminais no mundo altamente móvel de hoje, tornando os terminais alvos atraentes para ataques cibernéticos. Assim, a política de segurança deve se mover com usuários e dados e não deve ser vinculada a um local específico. (BRACH,2022, Disponível em: <https://www.securityreport.com.br/overview/)

Para MENDONÇA (2022), a implementação do MFA pode variar de acordo com o tamanho da organização, tecnologias, necessidades, entre outros fatores. Na Figura 1 apresenta-se as regras para gerir a autenticação adaptativa para permissão de login sobre o usuário para determinar os fatores de autenticação que serão aplicados, podem ser essas informações existem modelos diferentes de MFA, um exemplo é a autenticação adaptativa, a qual se utiliza de regras de:

Figura 1: Regras para gerir a autenticação adaptativa para permitir login.

Fonte: Elaboração própria, 2023.

Neste caso, ao efetuar o Login, é verificado o endereço de IP do dispositivo, qual o modelo do dispositivo e as demais informações. Segundo MENDONÇA (2022) todos esses dados são necessários para entender quais os riscos daquele acesso, pedindo a autenticação de dois fatores para que após a confirmação de todas as informações, o usuário consiga fazer login no sistema com segurança. Entretanto, esse tipo de identificação é o mais indicado, porém seu custo é elevado, então o mais comum é escolher um modelo predefinido que irá adotar autenticação padrão para todos os acessos.

Em concordância com MENDONÇA (2022), quando um sistema de MFA é utilizado, as camadas de segurança aumentam e se tornam mais concretas, dificultando a invasão de um cibercriminoso no sistema. O autor ainda afirma que “adotar o MFA significa garantir que os protocolos de segurança estejam mais fortalecidos, impedindo o acesso não autorizado à conta”.

Uma pesquisa feita pelo site Reclame Aqui em 2019, destinado a registrar reclamações diversas de clientes e usuários de diversos tipos de serviços e produtos, indicou que 88,6% dos usuários se preocupam com o uso de seus dados pelas organizações. Assim, a adoção de medidas de segurança como uso da autenticação multifator é extremamente positiva como forma de obter mais confiança dos usuários com seus sistemas, gerando um sentimento de satisfação entre eles.

Atualmente existem alguns métodos para burlar o MFA, porém grande parte deles podem ser evitados, eis alguns exemplos:

Ataques Man-in-the-Middle: Antes de explicar como funciona esse tipo de ataque, é importante ressaltar que uma boa parte dos ataques realizados contra o MFA se relacionam diretamente com a engenharia social, ou seja, a técnica de induzir o usuário a realizar uma ação que o possa prejudicar, como nesse caso, entrar em um site malicioso, o Homem-no-meio. Esse site por sua vez possui um proxy falso, que consegue ver tudo que o usuário digita, podendo assim roubar facilmente as credenciais de login e senha dele. Alternativamente, o homem-no-meio também pode capturar o cookie de acesso resultante, assim controlando a sessão.

Contudo, alguns métodos de MFA não podem ser burlados pelo homem-no-meio, como por exemplo o FIDO2. Esse tipo de ataque pode ser facilmente evitado verificando se o site em que o usuário está entrando é seguro, isso pode ser feito ao verificar se um “cadeado” aparece no canto superior esquerdo, indicando que o site acessado é seguro. A segurança do site também pode ser comprovada ao verificar se seu URL começa com “https”, já que o “S” significa “Seguro”.

Por fim, manter o software de segurança atualizado também ajuda a evitar esse tipo de ataque.

Ataques Man-in-the-End Point: Esse tipo de ataque é caracterizado pela presença de um malware no dispositivo, cujo infecta o dispositivo seja por engenharia social ou por uma brecha em um sistema operacional desatualizado. Esse modo se difere do homem-no-meio pois o malware espera até você abrir seu internet banking, por exemplo, e assim que seus dados fossem inseridos, ele abriria uma segunda sessão oculta no navegador para roubar seu dinheiro.

Assim como no homem-no-meio, para evitar o método de ataque homem-no-meio point basta verificar o URL do site e manter o software de segurança atualizado.

Autenticação falsa: Talvez o mais difícil de ser interrompido, esse método de ataque simula todo o processo de autenticação do MFA, desde a solicitação de usuário e senha até os outros fatores. Também conhecido como pescaria, neste método, o site malicioso em que essa autenticação está presente poderia pedir informações como número de cartão de crédito e poderia facilmente enganar o usuário por conta de sua perfeita simulação do MFA. Na maioria das vezes, a autenticação de multifator consegue se livrar desse tipo de ameaça, contudo, ter senhas fortes e diversificadas ajuda a evitar que esse tipo de ataque ocorra.

2.2. O estado da arte do MFA: Avaliação da eficácia do MFA em diferentes

setores e cenários de uso

De acordo com KASPERSKY (2022), a quebra de senha por força bruta é um método utilizado por hackers para descobrir senhas ao tentar todas as combinações possíveis até encontrar a senha correta. Para uma senha alfanumérica de 8 caracteres, existem várias combinações possíveis, e a força bruta pode ser um processo longo e demorado, dependendo dos recursos disponíveis para o invasor.

Se a senha contiver apenas caracteres alfabéticos (maiúsculos e minúsculos), sem números ou outros caracteres especiais, haverá 52 possibilidades de caracteres para cada posição da senha, o que significa que há 52^8 possíveis combinações de senhas. Isso equivale a aproximadamente 53 bilhões de combinações possíveis.

No entanto, se a senha incluir caracteres especiais, como números e símbolos, o número de possibilidades aumentará significativamente. Por exemplo, se a senha contiver letras maiúsculas e minúsculas, números e símbolos, haverá 94 possibilidades de caracteres para cada posição da senha, o que significa que há 94^8 possíveis combinações. Isso equivale a aproximadamente 6 quatrilhões de combinações possíveis.

Embora a força bruta possa eventualmente quebrar uma senha alfanumérica de 8 caracteres, o processo pode levar anos ou até décadas, dependendo da velocidade de processamento do hardware usado pelo invasor. A fim de proteger suas senhas, é recomendável usar senhas mais longas e complexas, além de alterá-las periodicamente, usar MFA mais do que duplica essa possibilidade e reduz drasticamente a possibilidade de um atacante ter êxito em sua missão, por isso os cibercriminosos tentam de outras artimanhas de invadir um sistema de maneira mais viável, contudo com o MFA essa “maneira mais viável” torna o trabalho mais árduo e quase ineficaz dependendo do tipo de fator usado na etapa de verificação de nível 2.

Sem o MFA, técnicas que envolvam qualquer tipo de quebra de segurança ficam mais fáceis, ainda mais se envolvem engenharia social, pois segundo ROCHA (2018) os brasileiros acessam em média oito links maliciosos por segundo (dados de 2018, Relatório DFNDR Lab.), sendo que destes, 66% são por meio do principal aplicativo de mensagens utilizado no Brasil, o WhatsApp. Este após infectado, de maneira generalizada, pode ver as senhas nas quais você teve de colocar para acessar determinado sistema, na qual sem o multifator fica bem fácil de

acessar.

O uso do MFA é recomendado em vários setores, especialmente em áreas onde há um alto risco de acesso não autorizado ou roubo de dados. No setor financeiro há serviços bancários e financeiros, onde o MFA é essencial para proteger as informações dos clientes e evitar fraudes. É comum que as instituições financeiras exijam o uso do MFA para acessar suas contas online ou realizar transações. Na saúde há informações pessoais e sensíveis dos pacientes, incluindo dados médicos e financeiros. O uso do MFA ajuda a proteger essas informações e evitar violações de privacidade. No quesito governamental, o MFA é usado para proteger informações confidenciais, como dados de cidadãos, segredos de estado e informações de inteligência. Nas instituições educacionais, o MFA é importante para proteger informações pessoais dos alunos, incluindo registros acadêmicos, dados financeiros e informações de identificação pessoal. Já no comércio eletrônico em lojas online e plataformas de comércio eletrônico, o MFA é importante para proteger informações de pagamento, evitar fraudes e garantir que os usuários estão autorizados a fazer compras.

Em resumo, o MFA é indispensável em setores que lidam com informações confidenciais e sensíveis, aos quais incluem inteiramente o escopo das finanças, saúde, governo, educação e comércio eletrônico.

2.3. Cenário Ideal

A junção de todas as etapas de segurança seria o ideal tornando uma invasão impossível, mas o investimento é elevadíssimo para se aplicar, dito isto, a aplicação de alguns MFA’s mais acessíveis já torna uma invasão quase que impossível. Assim como dito anteriormente, segundo MENDONÇA (2022) alguns cenários não requerem tanto a presença de um MFA de último nível, mas uma simples autenticação como o de um token de acesso, por exemplo, já é o suficiente para barrar mais do que a metade de tentativas de acesso ao um determinado sistema.

A Tabela 1 apresenta as etapas de autenticação obrigatórias ao multifator, uma vez que, para acessar uma devida conta do banco digital considera-se essas três etapas.

Tabela 1: Etapas de autenticação obrigatórias à autenticação multifator.

ETAPA 1	A primeira etapa, a etapa 1, que é a etapa do conhecimento, etapa 2 (posse) e etapa 3 (inerência), na etapa 1, ocorreria que, em vez da uma única senha de maneira padrão para acesso, teríamos várias perguntas de cunho pessoal (de conhecimento da pessoa e não necessariamente informações sensíveis) na qual resultariam em várias possibilidades de senhas na qual seria requisitado na tela de login de maneira aleatória, senha essa cuja a pessoa haveria respondido em forma de frase curta e simples mas não uma única palavra.
ETAPA 2	Na etapa 2, um objeto inteligente seria usado juntamente com um PIN para definir a localização e veracidade do autenticado.
ETAPA 3	E por fim e não menos importante, mas muito pelo contrário, na etapa final, a última prova de autenticação biológica e mais difícil de ser burlado por meios naturais, informações biométricas são coletadas a fim de serem igualmente como na etapa 1 pedidas de maneira aleatória, a fim de que, mesmo que o invasor tenha por qualquer meio algum dos fatores que o possam fazê-lo passar pelas etapas de segurança, o impeçam nesta em que se faz necessário o uso de informação única e precisa.

Para reforçar essa ideia de uma maneira simples, chega-se no esquema da Figura 2:

Certamente, com a etapa 2 já torna bem restrito a forma com a qual pode se realizar o acesso a determinado sistema, tornando uma forma de MFA muito útil, de forma acessível e segura. Como realizado anteriormente a conta das probabilidades de invasão por força bruta, as possibilidades de senha para 8 caracteres incluindo caracteres especiais e números é de 6 quatrilhões de combinações possíveis, nesse cenário, iniciando pela etapa 1, teríamos pelo menos 53 bilhões de possibilidades de senhas para cada pergunta, já na etapa dois, considerando que o invasor tenha descoberto a frase de segurança, pego o cartão da vítima (ou criado uma cópia) e passado adiante, existiria entre 10.000 e 100 milhões de combinações possíveis para o

PIN de confirmação, considerando mesmo assim o conhecimento e tecnologia avançada sobre a vítima e passado para a etapa final, está só seria possível devido ao sequestro da vítima, caso contrário a probabilidade de o invasor conseguir acesso ao sistema seria de 0%.

Figura 2: Esquema de login através das etapas de confirmação.

Fonte: Elaboração própria, 2023.

3. Algumas opções de MFA's existentes

Existem vários tipos de MFA, cada um com suas próprias vantagens e desvantagens em termos de segurança.

- Autenticação de dois fatores (2FA) com token de hardware físico é usado para gerar um código de acesso temporário que é usado juntamente com a senha do usuário para fazer login.
- O token é seguro porque usa um algoritmo criptográfico forte para gerar o código de acesso e é separado do dispositivo do usuário, o que torna difícil para um invasor obter acesso. É comumente utilizado por instituições financeiras para gerar um código de acesso, muito parecido com o botão de rádio frequência usado no acesso de condôminos para a liberação de entrada na controladoria de acesso.
- Já na 2FA de autenticação por push o usuário é solicitado a aprovar um login em seu dispositivo móvel ou computador, em vez de inserir um código de acesso. A autenticação por push é segura porque a solicitação de login é criptografada e enviada diretamente para o dispositivo do usuário, o que torna difícil para um invasor interceptar a solicitação. Autenticação multifatorial baseada em biometria como impressões digitais, reconhecimento facial ou reconhecimento de voz, são usadas como um fator de autenticação adicional.

- A autenticação baseada em biometria é segura porque as informações biométricas são únicas para cada usuário e difíceis de serem duplicadas por um invasor. Sua aplicação maior é no desbloqueio de telefones celulares, prático, ágil e seguro.
- A autenticação multifatorial baseada em aplicativo requer que um aplicativo de autenticação seja instalado no dispositivo móvel do usuário, que gera um código de acesso temporário que é usado juntamente com a senha do usuário para fazer login. Esse método é seguro porque o aplicativo de autenticação é protegido por senha e é difícil para um invasor obter acesso.

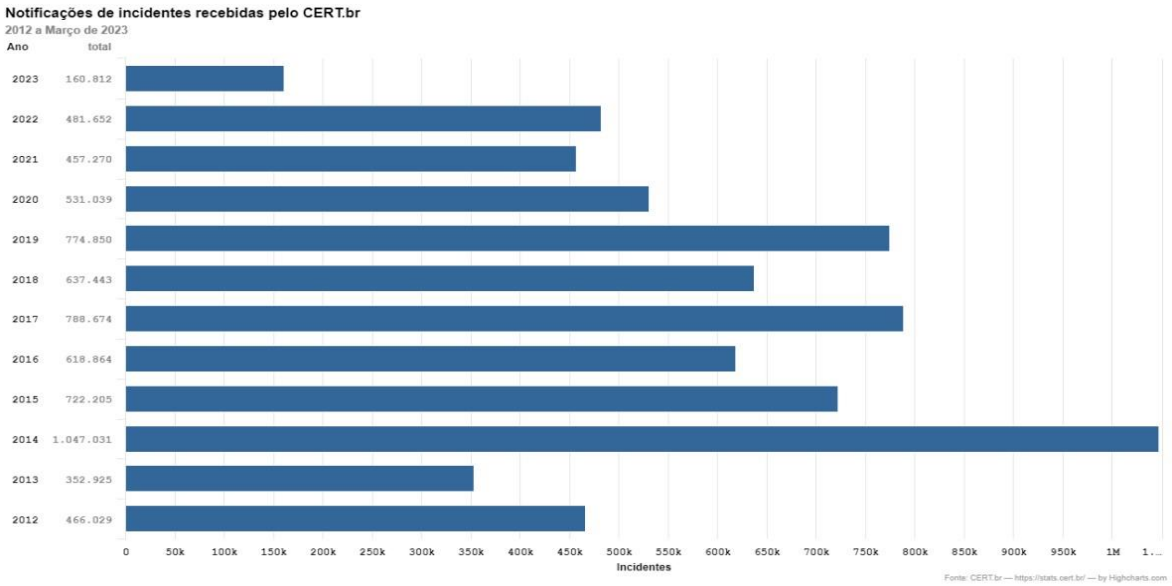
Autenticação multifatorial baseada em cartão inteligente é usada para armazenar as informações de autenticação do usuário. Para fazer login, o usuário insere ou aproxima o cartão inteligente em uma leitora e digita sua senha ou não, dependendo da tecnologia. Essa abordagem é segura porque as informações de autenticação do usuário são armazenadas no cartão inteligente, o que torna difícil para um invasor obter acesso.

E por fim a autenticação multifatorial baseada em voz permite que o usuário faça uma chamada telefônica para um sistema de autenticação que usa reconhecimento de voz para verificar a identidade do usuário. Esse método é seguro porque as informações de autenticação do usuário são verificadas por meio do reconhecimento de voz, que é muito difícil de ser falsificado.

Os métodos de autenticação multifatorial menos seguros são aqueles que podem ser mais facilmente comprometidos ou falsificados, e na maioria das vezes por erro humano, são eles: Autenticação multifatorial baseada em SMS, pois um código de acesso temporário é enviado para o dispositivo móvel do usuário por meio de mensagem de texto na qual o invasor pode utilizar-se da técnica do “homem no meio” para interceptar a informação antes da vítima ou por meio de clonagem. As mensagens de texto também podem ser interceptadas por meio de ataques de Troca do Módulo de Identificação do Assinante (“Sim Swapping”) ou de Pescaria ("phishing"), o que pode permitir que um invasor obtenha acesso ao código de acesso temporário. A autenticação multifatorial baseada em e-mail da mesma forma recebe um código de acesso temporário enviado para a caixa de entrada do correio eletrônico do usuário. No entanto, as contas de e-mail podem ser comprometidas por meio de ataques de pescaria ou

engenharia social, o que pode permitir que um invasor obtenha acesso ao código de acesso temporário. Inclusive é bem comum que isso aconteça tanto pessoal quanto em grandes corporações devido à falta de conscientização e treinamento especialmente, mas não unicamente, a pessoas de mais idade nas quais tem menos afeto com as novas tecnologias do mercado. Na Figura 3 observa-se o número de notificações de incidentes relatados ao CERT.BR, empresa de Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil que presta serviços da área de Gestão de Incidentes de Segurança da Informação para empresas de pequeno, médio e grande porte.

Figura 3: Incidentes relatados de 2012 a 2023.



Fonte: CERT.BR.

Autenticação multifatorial baseada em pergunta e resposta de segurança para fazer login podem ser facilmente adivinhadas ou obtidas por meio de engenharia social. Autenticação multifatorial baseada em token físico podem ser uma boa barreira de segurança, no entanto, os tokens físicos podem ser perdidos ou roubados, o que pode permitir que um invasor obtenha acesso ao código de acesso temporário.

Além disso, é importante destacar que a segurança do MFA também depende do comportamento do usuário com dito anteriormente. Por exemplo, se o usuário compartilhar suas credenciais de autenticação, ou utilizar senhas fracas e fáceis de adivinhar, mesmo com a autenticação multifatorial, sua conta ainda estará vulnerável a ataques.

Outro fator importante é que alguns métodos de autenticação multifatorial podem ser mais adequados para determinados tipos de usuários ou ambientes. Por exemplo, um token físico pode ser mais adequado para um ambiente corporativo em que o usuário possui um local seguro para armazenar o token, enquanto a autenticação baseada em SMS pode ser mais adequada para usuários em geral que desejam proteger sua conta em serviços online.

Portanto, a escolha do método de autenticação multifatorial mais seguro deve levar em consideração não apenas a tecnologia envolvida, mas também o comportamento do usuário e as necessidades específicas do ambiente em que será usado.

4. O grande problema

Embora o MFA possa parecer maravilhoso, sempre existe algo por trás que pode acabar com todo o esquema de segurança de maneira “bem simples e rápida”. E sim, estamos falando do problema que na maioria dos casos de vazamentos de dados e invasões cibernéticas é o causador, o ser humano.

Para algumas pessoas, em especial as com idade mais avançadas, podem ficar com medo, enfrentar dificuldades, ou até mesmo retirar essa segurança só por se tratar de algo enfadonho e querer o caminho mais simples ao acessar uma conta da rede social por exemplo.

Apesar do MFA ser uma tecnologia de segurança muito eficaz, há algumas desvantagens que podem ser levadas em consideração como mostrado na Tabela 2:

Tabela 2: Desvantagens do MFA.

Investimento em hardware e software	A implementação do MFA pode exigir investimentos em hardware e software, além de um esforço significativo de desenvolvimento e manutenção Curva de aprendizado para os usuários
Curva de aprendizado para os usuários	O MFA exige que os usuários aprendam novos métodos de autenticação, o que pode ser confuso e levar tempo para se acostumarem já que como dito anteriormente, preferem o caminho mais curto

Disponibilidade de conexão de rede	Alguns métodos de autenticação do MFA exigem uma conexão de rede confiável, o que pode ser um problema em áreas remotas ou em emergências
Interação do usuário	Alguns métodos de autenticação do MFA exigem uma interação do usuário, como responder a uma pergunta de segurança ou escanear um código QR, o que pode ser um incômodo para alguns usuários
Vulnerabilidades específicas	Alguns métodos de autenticação MFA, como senhas de aplicativo ou tokens de hardware, podem apresentar vulnerabilidades específicas que precisam ser levadas em consideração ao implementar o MFA. Algumas podem simplesmente serem resolvidas com atualizações de segurança e outras necessitam de uma equipe especializada para identificar o problema e obliterá-lo
Dependência de terceiros	Algumas implementações de MFA exigem que as empresas dependam de provedores de autenticação de terceiros, o que pode ser um problema se esses provedores tiverem problemas técnicos ou de segurança Maior complexidade
Maior complexidade	A implementação do MFA pode tornar a autenticação mais complexa, o que pode levar a erros de autenticação e dificuldades para os usuários
Incompatibilidade com alguns sistemas	Algumas implementações de MFA podem não ser compatíveis com todos os sistemas e aplicativos, o que pode limitar sua capacidade de serem usados em ambientes de trabalho específicos
Falhas técnicas	Como qualquer tecnologia, o MFA pode apresentar falhas técnicas que podem impedir os usuários de acessarem seus sistemas e aplicativos Atrasos de autenticação
Atrasos de autenticação	Em alguns casos, o MFA pode levar a atrasos na autenticação, o que pode ser um problema em emergências ou quando há necessidade de acesso imediato Requisitos de manutenção
Requisitos de manutenção	A implementação do MFA pode exigir requisitos adicionais de manutenção, como a substituição de tokens de hardware ou a atualização de software Problemas de privacidade

Problemas de privacidade	Alguns métodos de autenticação MFA, como biometria, podem levantar preocupações de privacidade se não forem implementados de forma segura e responsável

Apesar dessas desvantagens, o MFA ainda é amplamente considerado uma das melhores formas de aumentar a segurança de autenticação em sistemas e aplicativos online, tendo como principal preocupação o ser humano e como ele lida com esse tipo de camada extra de segurança, uma vez que se faz necessário mais segurança devido aos altos índices de ataque cibernética que aumentam cada vez mais atualmente, e que esse tipo de tecnologia pode ajudar (e muito) na prevenção de invasão. Como qualquer outra tecnologia, o MFA pode ter suas desvantagens dependendo muito de sua aplicação e seu ambiente de desenvolvimento, porém exuma-se a culpa de uma possível invasão a ela, pois é mais provável que uma invasão ocorra devido a falha humana do que a de um outro fator de autenticação de segurança.

Por isso é tão importante o treinamento de todo aquele que faz uso de um aparelho que pode ser infectado e devastar uma rede de equipamentos inteira por falta de conhecimento ou treinamento de pessoal.

5. Conclusão

Atualmente, especialmente no ambiente corporativo, mas não se limitando a este, é essencial que estejamos cientes de todas as camadas de proteção disponíveis no mercado, uma vez que as informações são um dos ativos mais valiosos de uma empresa, e da mesma maneira deve ser para cada indivíduo, os detentores dessas informações, zelar e cuidar de como os usam, pois com elas é possível realizar inúmeras ações, principalmente, mas não exclusivamente se passar por outra pessoa para cometer crimes.

Conforme explicado na seção 1, o multifator de autenticação é e será cada vez mais indispensável no quesito segurança, de maneira simples e eficaz é possível prevenir uma possível tentativa de invasão por meio qualquer técnica de invasão, mesmo que para isso seja necessário o aborrecimento de alguns usuários, pois faz jus seu uso.

Em seguida, pôde-se comprovar que o ataque por força bruta é possível, entretanto, com o MFA torna-se ineficaz devido que torna necessário autenticar-se por pelo menos um dos

meios existentes da autenticação por multifator. Em um cenário ideal, a aplicação de todos os meios possíveis de autenticação multifatorial seria uma excelente barreira de segurança que reduziria a 0% a chance de invasão sem os meios físicos como extorsão ou sequestro da vítima, contudo como seu custo é elevadíssimo, é importante levantar quais são os meios de autenticação mais seguros e qual é possível implantar conforme a necessidade e dentro do orçamento estipulado.

Referências

ARMANI, Victor. Benefícios da Autenticação Multifator (MFA). Disponível em: https://tripla.com.br/autenticacao-multifator-mfa/. Acesso em 15 nov. 2022.

BRACH, Dennis. Importância da MFA em uma estrutura de segurança, endpoint e Zero Trust. Disponível em: https://www.securityreport.com.br/overview/importancia-da-mfa-em-umaestrutura-de-seguranca-endpoint-e-zero-trust/#.Y3OL9eTMKUl. Acesso em 15 nov. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018.

CAETANO, Érica. O que é hacker?. Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm. Acesso em 05 de maio de 2023.

CETAX. Big Data: O que é, conceito e definição. Cetax. Disponível em: https://cetax.com.br/big-data/. Acesso em 05 de maio de 2023.

FALCÃO, Flávia. O uso de MFA e sua importância dentro de uma empresa. Disponível em: https://www.trustcontrol.com.br/blog/o-uso-de-mfa-e-sua-importancia-dentro-de-umaempresa/. Acesso em 15 nov. 2022.

KASPERSKY. Como se defender de ataques do tipo “man-in-the-middle”. Disponível em: https://www.kaspersky.com.br/resource-center/threats/man-in-the-middle-attack. Acesso em 16 nov. 2022.

KASPERSKY. O que é um ataque de força bruta?. Kaspersky. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/brute-force-attack. Acesso em 05 de maio de 2023.

MARTINS, Renato. Segurança da informação: como proteger os dados na sua empresa contábil. Conta Azul. Disponível em: https://contadores.contaazul.com/blog/seguranca-dainformacao. Acesso em 05 de maio de 2023.

MENDES, Francisco Schertel; CARVALHO, Vinícius Marques de. Compliance: concorrência

e combate à corrupção. São Paulo: Trevisan Editora, 2017, p. 31.

MENDONÇA, Diego. O que é MFA e por que as empresas tem adotado? Disponível em: https://levva.io/o-que-e-mfa-e-por-que-as-empresas-tem-adotado/. Acesso em 15 nov. 2022.

ORACLE. O que é Big Data?. Oracle. Disponível em: https://www.oracle.com/br/bigdata/what-is-big-data/#best-practices. Acesso em 05 de maio de 2023.

QUINTANILHA, Ariana Miranda. A LGPD como um pilar do compliance. Disponível em: https://www.conjur.com.br/2022-mai-17/ariana-quintanilha-lgpd-pilar-compliance. Acesso em 16 nov. 2022.

ROCHA, Douglas. ENGENHARIA SOCIAL: COMPREENDENDO ATAQUES E A IMPORTÂNCIA DA CONSCIENTIZAÇÃO. Disponível em: https://meuartigo.brasilescola.uol.com.br/atualidades/engenharia-social compreendendoataques-importancia-conscientizacao.htm. Acesso em 07 de abr. 2023.

VIANA, Rafael. O que é e como funciona a MFA (Autenticação Multifator)? Disponível em: https://www.caf.io/post/o-que-e-mfa-autenticacao-multifator. Acesso em 15 nov. 2022.