SEGURANÇA ALÉM DOS MUROS DAS ORGANIZAÇÕES

TADEU WOHLERS GÂMBARO LIMA[1]
CLAYTON EDUARDO DOS SANTOS[2]

RESUMO

A autenticação de usuários em sistemas de informação é um dos pontos mais delicados dos mesmos, pois uma vez validados, dependendo dos privilégios, eventualmente podem ter acesso a recursos que talvez não deveriam. A utilização de múltiplos fatores de autenticação, tem sido uma das soluções para este tipo de problema, sendo um recurso cada vez mais utilizado para proteger as organizações de ataques informáticos. O mesmo é baseado na premissa de que um terceiro não autorizado pode não ser capaz de fornecer os elementos necessários para uma camada adicional de autenticação, necessária para o efetivo acesso. Se em uma tentativa de autenticação pelo menos um dos componentes estiver ausente ou fornecido incorretamente, a identidade do usuário não é validada e o acesso aos recursos, que eventualmente seriam liberados na etapa de autorização, negado. O presente trabalho tem como objetivo discorrer sobre os meios utilizados para a elevação da segurança dos dados nas organizações, em ambiente interno e externo, bem como o uso de ferramentas baseadas em Fator de Autenticação adicional, pode criar uma barreira sólida na proteção das informações.

Palavras-chave: autenticação de dois fatores. segurança de dados. segurança de informação.

[1] Especialização em Gestão Estratégia de Tecnologia da Informação | Câmpus Bragança Paulista do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo. Curso de Pós-Graduação Lato Sensu (IFSP). E-mail: tadeu.wohlers@gmail.com.
[2] Professor Titular | Câmpus Bragança Paulista do Instituto Federal de Educação, Ciência e Tecnologia de São Paulo (IFSP). E-mail: claytones@ifsp.edu.br.

SECURITY BEYOND THE WALLS OF ORGANIZATIONS

ABSTRACT

Authentication of users in information systems is one of their most delicate points, as once validated, depending on the peculiarities, they may eventually have access to resources that they perhaps should not. The use of multiple authentication factors has been one of the solutions to this type of problem, being a resource increasingly used to protect organizations from computer attacks. The same is based on the requirement that an unauthorized third party may not be able to provide the necessary elements for an additional layer of authentication, necessary for effective access. If in an authentication attempt at least one of the components is missing or incorrectly provided, a user's identity is not validated and access to resources, which may eventually be released in the authorization stage, is denied. The present work aims to disagree on the means used to increase data security in organizations, in internal and external environments, as well as the use of tools based on the additional Authentication Factor, which can create a solid barrier in the protection of information.

Keywords: *Data security. Two-factor authentication. Information security.*

1. INTRODUÇÃO

Na era digital, a segurança da informação tornou-se um tema crucial, à medida que a sociedade se torna cada vez mais dependente de sistemas digitais interconectados. Com o advento da computação em nuvem, "*Internet* das Coisas" (IoT) e o aumento da utilização de aplicativos e serviços online, a segurança não pode mais ser encarada apenas como uma preocupação interna das organizações, devendo ser considerada além dos limites físicos de seus próprios muros, afinal, toda organização necessita compartilhar dados com o mundo externo.

A proteção de dados, a privacidade e a confidencialidade das informações se tornaram desafios complexos, pois os sistemas digitais estão interligados em uma ampla rede de comunicação, em constante expansão e evolução. A segurança desses sistemas não pode mais ser tratada isoladamente pelas organizações, pois requer uma abordagem integrada e colaborativa entre diferentes atores.

O objetivo do presente trabalho é explorar a segurança além dos muros das organizações, abordando as questões relacionadas à identidade e proteção de sistemas digitais e dados em um contexto mais amplo. Neste contexto, "além dos muros" refere-se a um ambiente que vai além dos limites geográficos de uma organização específica e envolve a interação com sistemas, redes, aplicativos externos e compartilhamento de dados, nos quais a confiabilidade e a integridade da informação são fundamentais.

Será realizada uma análise dos desafios e ameaças à segurança em sistemas digitais, discutindo as medidas e estratégias que podem ser adotadas para garantir a segurança nesse ambiente expandido. Será abordado também como o uso de Múltiplos Fatores de Autenticação (MFAs) adicionam uma importante camada extra de proteção.

Além disso, será abordada a importância do gerenciamento de identidade e acesso como uma medida essencial para fortalecer a segurança das organizações no contexto supracitado. Por fim, será apresentado um estudo de caso hipotético, de uma empresa que possui filiais em algumas cidades e faz uso de sistemas em nuvem para

o compartilhamento de dados entre a matriz e as referidas unidades, bem como, com outras empresas parceiras do seu ecossistema.

Espera-se que este estudo contribua para a compreensão das complexidades envolvidas na segurança em um mundo digitalmente interconectado, fornecendo *insights* valiosos para a proteção de sistemas digitais dentro e fora das organizações.

2. FUNDAMENTAÇÃO TEÓRICA

Com o aumento da performance dos dispositivos computacionais tradicionais, bem como das alternativas disponíveis nos diferentes paradigmas de computação distribuída disponíveis na atualidade, as senhas passam a despertar cada dia mais, a atenção de administradores de sistemas e usuários mal intencionados, dada a premissa de que um sistema computacional, responsável por validar transações ou acessar recursos, desempenha tal papel em especial, por meio do fornecimento de uma senha por parte do usuário. As organizações dependem da robustez do sistema de autenticação e da sua infraestrutura, de modo que, se um atacante conseguir quebrar este mecanismo, terá acesso aos recursos que devem ser protegidos.

Isso ocorre porque na prática, as senhas são um segredo compartilhado, uma chave que “prova” que quem a possui é, quem diz ser, de modo que, uma vez autenticado, tal portador passa a ter autorização compatível com o perfil informado e consequentemente, pode executar certas transações. Não é razoável continuar pedindo aos usuários que reforcem ainda mais suas senhas, que devem ter pelo menos 12 caracteres, uma letra minúscula, uma maiúscula, um ou mais caracteres especiais, ao menos um número que não seja escalonado, além de não fazer menção a eventuais dados pessoais do usuário, como a data de nascimento, por exemplo.

A segurança em sistemas digitais é de suma importância para garantir a proteção das informações contra acessos não autorizados, uso indevido, alteração ou destruição de dados. A segurança deve ser uma preocupação fundamental em todos os níveis dos sistemas, desde a infraestrutura de rede até os aplicativos e dispositivos utilizados.

Para compreender a natureza das ameaças e desafios enfrentados na segurança em sistemas digitais, é necessário ressaltar a necessidade de um enfoque multidimensional. Isso implica considerar não apenas as vulnerabilidades técnicas, mas também aspectos humanos, organizacionais e sociais que podem comprometer a segurança.

A proteção adequada dos sistemas digitais requer o entendimento das diversas ameaças que podem comprometer a segurança do usuário. As ameaças são cada vez mais sofisticadas, com *hackers* explorando vulnerabilidades e técnicas avançadas para acessar informações sensíveis.

Aplicações *web* e móveis são frequentemente alvos de ataques, o que exige medidas de segurança eficazes para proteger os dados dos usuários. Vulnerabilidades, como injeção de código e *cross-site scripting* (XSS), podem ser exploradas por atacantes para comprometer a integridade e a confidencialidade das informações.

Para mitigar esses riscos, é necessário, dentre outras medidas, adotar boas práticas de desenvolvimento seguro, como validação de entrada de dados e sanitização de saída.

O gerenciamento de identidade e acesso desempenha um papel crítico na segurança das organizações, independentemente da localização física do usuário, característica típica em tempos de mobilidade, expansão das redes móveis de banda larga e trabalho remoto.

A autenticação multifatorial (MFA) é uma técnica poderosa para fortalecer a identificação dos usuários, exigindo a apresentação de múltiplos fatores de autenticação. MFAs utilizam testes para poder validar corretamente a transação solicitada, agrupando-os em fatores de diferentes tipos e classificando-os para poder estudá-los melhor, podendo por fim, definir com mais clareza as premissas ou requisitos que um verificador deve ter para realizar a autenticação multifator.

> A autenticação de dois fatores é um recurso oferecido por vários prestadores de serviços online que acrescentam uma camada adicional de segurança para o processo de *login* da conta, exigindo que o usuário forneça duas formas de autenticação. A primeira forma – em geral – é a sua senha. O

> segundo fator pode ser qualquer coisa, dependendo do serviço. O mais comum dos casos, é um *SMS* ou um código que é enviado para um *e-mail.* A teoria geral por trás de dois fatores é que para efetuar login, você deve saber e possuir algo a mais. (RODRIGUES, 2022, p. 01)

Começaremos com uma pequena classificação para entender como os fatores são divididos para autenticar: baseado em algo que o usuário conhece, por exemplo uma senha, datas de nascimento, o nome do primeiro animal de estimação; baseado em algo que possui como por exemplo um cartão de crédito, certificado digital; ou ainda, dados com base em alguma característica física ou ato involuntário do indivíduo, como uma impressão, padrões de escrita, voz ou oculares – os chamados dados biométricos.

O *Single Sign-On* (SSO) permite que os usuários acessem diversos sistemas com um único conjunto de credenciais, reduzindo a exposição a ataques de senha. O *Identity as a Service* (IDaaS) oferece soluções baseadas em nuvem para o gerenciamento seguro de identidades e acesso.

3. SEGURANÇA EM AMBIENTES DE NUVEM

3.1. Modelo de Responsabilidade Compartilhada

Segundo Miranda (2021) é fundamental ressaltar que a segurança dos dados na nuvem é uma responsabilidade compartilhada entre o fornecedor dos serviços e o cliente, e varia de acordo com o modelo adotado ao provisionar recursos na nuvem. O modelo de responsabilidade compartilhada é um conceito importante na área da segurança da informação e está diretamente relacionado ao tema de "Segurança além dos muros das organizações". Nesse sentido vale lembrar que:

> Esse modelo de responsabilidade compartilhada entre o cliente e a AWS também se estende aos controles de TI. Assim como a responsabilidade para operar o ambiente de TI é compartilhada entre a AWS e os seus clientes, o mesmo ocorre com o gerenciamento, a operação e a verificação de controles compartilhados de TI. A AWS pode auxiliar a reduzir os encargos operacionais de controles do cliente gerenciando os controles associados à infraestrutura física implementada no ambiente da AWS que anteriormente

> eram gerenciados pelo cliente. Já que cada cliente é implantado de forma diferente na AWS, os clientes podem aproveitar a transferência do gerenciamento de determinados controles de TI para a AWS, resultando em um (novo) ambiente de controle distribuído. Os clientes podem usar a documentação sobre controle e conformidade da AWS para executar seus procedimentos de avaliação e verificação de controle, conforme for necessário. (AMAZON, 2023, texto online).

Esse modelo se refere à distribuição das responsabilidades e tarefas relacionadas à segurança entre diferentes entidades, como provedores de serviços, empresas, usuários e governos, em um ecossistema digital interconectado. O conceito de responsabilidade compartilhada reconhece que a segurança não é apenas uma preocupação exclusiva das organizações que oferecem produtos ou serviços digitais, mas é uma responsabilidade que deve ser dividida com todos os envolvidos na utilização desses recursos.

Essa abordagem colaborativa busca garantir uma proteção mais abrangente dos dados e informações, considerando que cada participante tem um papel fundamental a desempenhar na manutenção de um ambiente seguro. Dentro do contexto da segurança em sistemas digitais, podemos analisar o modelo de responsabilidade compartilhada sob diferentes perspectivas:

Provedores de Serviços e Empresas

Os provedores de serviços e empresas que oferecem produtos e aplicativos digitais devem assumir a responsabilidade de garantir a segurança dos sistemas e dados que estão sob sua gestão. Isso envolve implementar medidas de proteção adequadas, como criptografia, controle de acesso, monitoramento de atividades suspeitas e atualizações regulares para corrigir vulnerabilidades.

Usuários

Os usuários também têm uma parte importante na responsabilidade compartilhada. Eles devem estar cientes das práticas recomendadas de segurança,

como a criação de senhas fortes, o uso de autenticação multifatorial e a adoção de boas práticas de navegação segura.

A conscientização e a educação dos usuários são fundamentais para evitar práticas negligentes que possam expor seus dados pessoais e informações confidenciais.

Governos e Reguladores

Os governos desempenham um papel significativo na garantia da segurança cibernética em nível nacional e internacional. Estes devem estabelecer políticas, regulamentos e leis que incentivem e exigem boas práticas de segurança por parte das organizações e dos cidadãos. Além disso, devem investir em iniciativas de conscientização e educação para aumentar a segurança em toda a sociedade.

Parcerias e Colaborações

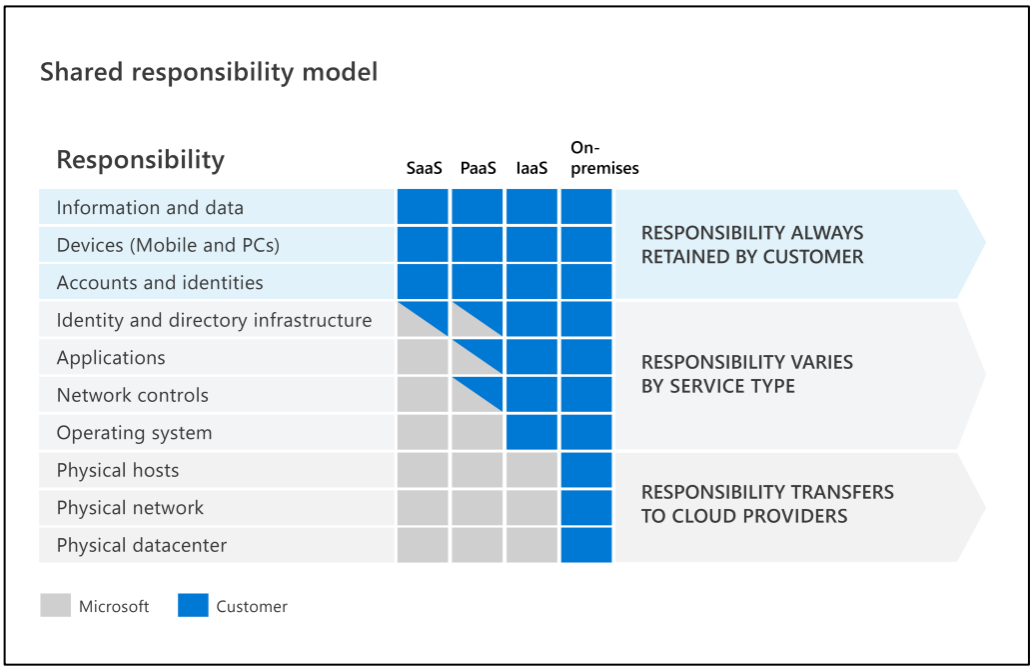
A responsabilidade compartilhada também pode envolver parcerias e colaborações entre diferentes entidades para combater ameaças cibernéticas. Isso pode incluir o compartilhamento de informações sobre ameaças, práticas recomendadas de segurança e a colaboração em iniciativas de resposta a incidentes de segurança. As responsabilidades também variam de acordo com o tipo de serviço contratado:

- *Software as a Service* (SaaS);
- *Platform as a Service* (PaaS);
- *Infrastructure as a Service* (IaaS).

On-premises datacenter

A tabela abaixo mostra como a *Microsoft* compreende o modelo de responsabilidade compartilhada entre ela e seus clientes, a partir dos serviços oferecidos na plataforma *Azure*:

Imagem 01



Fonte: www.microsoft.com. Acesso: 10/08/2023.

Para todos os tipos de implantação de nuvem, o cliente possui seus dados e identidades. O cliente é responsável por proteger a segurança de seus dados, identidades e recursos locais, incluindo dispositivos móveis, PCs, impressoras e muito mais.

Já os outros recursos como aplicações, controle de rede e sistemas operacionais são de responsabilidade do cliente dependente do serviço contratado, como por exemplo um serviço do tipo *on-premise*. Outros tipos de serviços, implementados como PaaS, por exemplo, podem ter a responsabilidade

compartilhada. E finalmente serviços do tipo SaaS são de total responsabilidade da *Microsoft*.

3.2. Segurança em profundidade

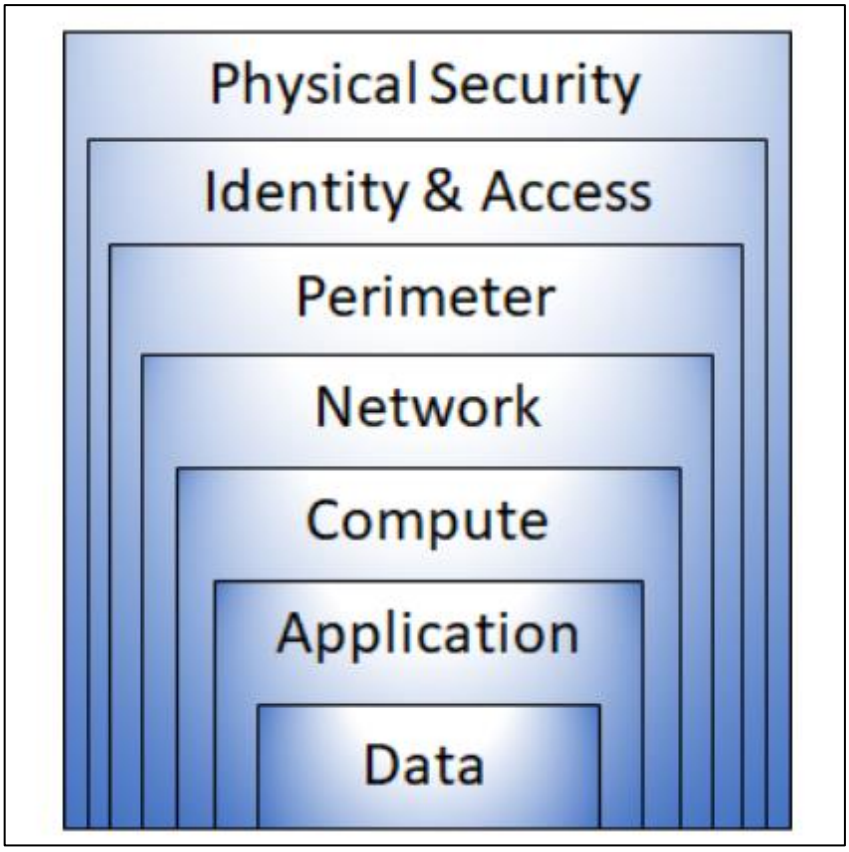
Segurança em profundidade, também conhecida como defesa em profundidade ou "*defense in depth*" em inglês, é uma estratégia de segurança da informação que tem como objetivo proteger sistemas, redes e informações por meio de múltiplas camadas de defesa.

> O valor da Defesa em Profundidade é a abordagem para combinar ferramentas avançadas de segurança para proteger dados cruciais e bloquear ameaças antes que elas atinjam endpoints e redes. A proteção de terminais, incluindo antivírus e firewalls, continua a ser o elemento fundamental de uma segurança completa; mas uma estratégia ampla de Defesa em Profundidade tem sido adotada cada vez mais, já que esses métodos de segurança de rede sozinhos já não são suficientes para proteger a força de trabalho moderna. (AVAST.COM, 2023, texto online).

Essa abordagem busca criar uma barreira robusta contra ameaças e ataques, garantindo que, caso uma camada seja comprometida, ainda haja outras linhas de defesa para impedir que o ataque avance ou cause danos significativos. A ideia central da segurança em profundidade é não depender exclusivamente de uma única medida de segurança, mas adotar várias camadas complementares, cada uma com sua própria função específica de proteção.

Essas camadas de segurança podem abranger aspectos tecnológicos, processuais e humanos. Dessa forma, mesmo que uma vulnerabilidade seja explorada ou uma defesa seja contornada, outras camadas estarão preparadas para impedir o avanço do ataque.

Imagem 02



Fonte: googleimagens.com. Acesso em: 10/08/2023

A imagem acima mostra um exemplo de segurança em camadas, onde a camada mais externa se remete à camada física, de infraestrutura, e a camada mais interna se refere aquilo que as organizações possuem de mais valioso, o dado. É possível observar que no modelo apresentado existem sei camadas que podem e devem ser protegidas, até que se chega na camada do dado, que também deve estar protegida.

3.3. Modelo *Zero Trust*

O modelo *Zero Trust* (confiança zero) é uma abordagem de segurança cibernética que se baseia na premissa de que nenhum usuário ou dispositivo deve ser confiável automaticamente, independentemente de sua localização ou origem. Ao

contrário dos modelos tradicionais de segurança baseados em perímetros, em que os dispositivos dentro de uma rede confiável são tratados como seguros, o modelo *Zero Trust* assume uma postura mais rigorosa, exigindo autenticação, autorização e verificação contínuas para todos os usuários e dispositivos, independentemente de estarem dentro ou fora da rede corporativa.

> *Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify."*
> *In a Zero Trust model, every access request is strongly authenticated, authorized within policy constraints and inspected for anomalies before granting access. Everything from the user's identity to the application's hosting environment is used to prevent breach. We apply micro-segmentation and least privileged access principles to minimize lateral movement. Finally, rich intelligence and analytics helps us identify what happened, what was compromised, and how to prevent it from happening again. (MICROSOFT, 2010, p. 02).*

A ideia fundamental do modelo *Zero Trust* é que todas as comunicações e interações devem ser autenticadas e autorizadas antes de serem permitidas. Isso é especialmente relevante em um cenário de ameaças cibernéticas cada vez mais sofisticadas e em uma era em que as organizações estão cada vez mais adotando ambientes de nuvem, dispositivos móveis e acesso remoto.

O modelo é baseado em 3 princípios guias:

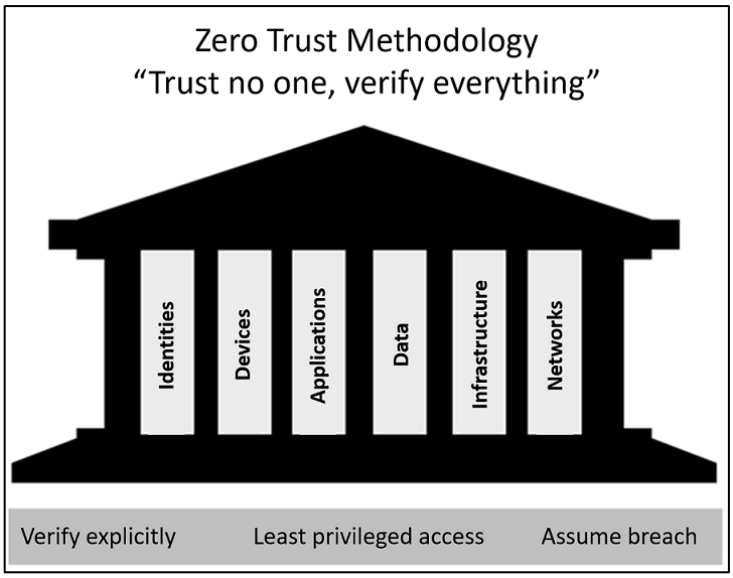
- Verificação explícita;
- Menor privilégio de acesso;
- Segmentação de acesso.

E possui 6 pilares fundamentais:

- Identidade;
- Dispositivos;
- Aplicações;
- Dados;

- Infraestrutura;
- Rede.

Imagem 03



Fonte: www.microsoft.com. Acesso: 10/08/2023.

Benefícios do modelo *Zero Trust*

- Maior Segurança: A abordagem *Zero Trust* ajuda a reduzir significativamente a superfície de ataque e a mitigar os riscos de violações de segurança, pois requer verificação contínua de identidades e comportamentos.

- Proteção em Ambientes Distribuídos: Com o aumento do trabalho remoto e ambientes de nuvem, o modelo *Zero Trust* oferece uma proteção mais eficiente contra ameaças em redes distribuídas e descentralizadas.

- Adaptação a Novos Desafios: Em um cenário de segurança em constante evolução, o modelo *Zero Trust* permite que as organizações se adaptem a novas ameaças e desafios de forma mais ágil.

3.4. Gerenciamento de Identidade de Acesso

O gerenciamento de identidade é uma área essencial na segurança da informação e se concentra em estabelecer e manter identidades digitais confiáveis para usuários, dispositivos e serviços em um ambiente computacional. Essa prática é crucial para garantir que as pessoas certas tenham acesso às informações e recursos adequados, enquanto impede o acesso não autorizado e protege a privacidade dos usuários.

Principais elementos do gerenciamento de identidade

- Autenticação: O processo de autenticação verifica a identidade de um usuário ou dispositivo por meio de credenciais, como senhas, *tokens*, chaves ou biometria. A autenticação garante que apenas usuários legítimos possam acessar um sistema ou serviço.

- Autorização: Uma vez autenticado, o usuário ou dispositivo recebe permissões adequadas com base em seu papel e privilégios. A autorização garante que o acesso seja restrito apenas ao que é necessário para realizar suas tarefas.

- Diretórios de Identidade: São sistemas que armazenam informações sobre usuários e dispositivos, como nomes, senhas criptografadas, atributos e permissões. Os diretórios de identidade são usados para centralizar e gerenciar informações de identidade.

- *Single Sign-On* (SSO): O SSO é uma abordagem que permite que os usuários façam login uma vez e acessem várias aplicações ou serviços sem a necessidade de autenticação repetida. Isso melhora a experiência do usuário e reduz o número de senhas a serem lembradas.

- Multifator de Autenticação (MFA): O MFA exige que os usuários forneçam mais de uma forma de autenticação, como algo que sabem (senha), algo que têm (*token*) e algo que são (biometria). Essa abordagem fortalece a segurança em comparação com a autenticação com um único fator (por exemplo, senha).

- Provisionamento de Identidade: O provisionamento de identidade trata do processo de criar, atualizar ou remover contas de usuários e dispositivos em sistemas e aplicativos. Uma abordagem eficiente de provisionamento garante que as alterações sejam refletidas corretamente em todas as plataformas.

- Desativação de Contas: O gerenciamento de identidade também inclui a desativação ou exclusão de contas de usuários ou dispositivos quando não são mais necessárias ou quando um usuário deixa uma organização. Isso ajuda a mitigar riscos de acesso não autorizado.

Benefícios do gerenciamento de identidade

- Maior Segurança: O gerenciamento de identidade ajuda a garantir que apenas usuários legítimos tenham acesso aos sistemas e informações, reduzindo os riscos de violações de segurança.

- Conformidade: Muitas regulamentações e normas de segurança exigem o controle rigoroso de acesso e gerenciamento de identidades para proteger dados sensíveis.

- Experiência do Usuário Aprimorada: Com recursos como *Single Sign-On* (SSO), os usuários têm uma experiência mais fácil e consistente ao acessar vários serviços.

3.5. Utilização de Múltiplos Fatores de Autenticação (MFA)

Na segurança informática, é preciso tentar alcançar um equilíbrio entre o que é amigável e o que é seguro, pois pode correr o risco de ter um sistema muito seguro, mas que ninguém quer usá-lo. Atualmente existem empresas que fornecem soluções de autenticação de três fatores, mas que permitem ao testador validar dois dos três testes.

Isso geralmente torna o sistema mais inseguro do que um dos dois fatores, pois há mais uma variável que pode ser comprometida. Os requisitos de segurança da indústria e os regulamentos estão mudando constantemente para responder às ameaças emergentes, e é por isso que talvez no futuro existam verificadores com mais de dois fatores de autenticação.

De fato, existem caixas eletrônicos que validam o testador biometricamente, através de suas impressões digitais, não seria difícil pensar que este último fator é necessário apenas para operações mais importantes, como extrações ou transferências de dinheiro.

O uso de múltiplos fatores de autenticação (MFA), também conhecido como autenticação multifator, é uma abordagem de segurança que exige que os usuários forneçam mais de uma forma de comprovação de identidade para acessar um sistema ou serviço.

> A autenticação de dois fatores não é um método infalível, mas é uma excelente barreira para prevenir a intromissão indesejada nas suas contas online. É de conhecimento público que as senhas são uma faca de foi de gumes: as mais fracas são fáceis de lembrar, mas são muito fáceis de serem adivinhadas. E as fortes podem ser difíceis de adivinhar, mas também são difíceis de lembrar. Devido a isso, as pessoas que já são ruins na criação de senhas, utilizam a mesma para todas as suas contas. Nesse sentido, a autenticação de dois fatores, pelo menos, faz com que seja um cibercriminoso não só tenha que descobrir sua senha, como também acessar o segundo fator, muito mais difícil de conseguir e, que implicaria roubar um telefone celular ou assim comprometer uma conta de e-mail. (RODRIGUES, 2022, p. 01-02).

Ao combinar diferentes fatores de autenticação, o MFA torna mais difícil para invasores comprometerem contas, pois um único fator (como uma senha) não é suficiente para conceder acesso. Existem três categorias principais de fatores de autenticação:

- Fator de Conhecimento: Essa categoria abrange fatores que se baseiam no que o usuário sabe, como senhas, códigos *PIN* ou respostas a perguntas de segurança. Senhas são os fatores de autenticação mais comuns, mas também podem ser suscetíveis a ataques de força bruta ou adivinhação. Um exemplo é a senha em que o usuário digita uma combinação de caracteres conhecida apenas por ele para acessar uma conta.

- Fator de Posse: Os fatores de autenticação desse grupo envolvem algo que o usuário possui, como dispositivos móveis, *tokens* de autenticação físicos ou virtuais, ou *smart cards*. Esses dispositivos geram códigos temporários ou únicos que são usados durante o processo de autenticação. Um exemplo é o *token* de autenticação em que o usuário recebe um *token* que gera um código numérico que muda a cada poucos segundos. Esse código é inserido durante o processo de autenticação.

- Fator de Inerência: Esses fatores são baseados em características físicas ou comportamentais do usuário, como impressões digitais, reconhecimento facial ou padrões de digitação. Esse tipo de autenticação é comum em dispositivos biométricos. Um exemplo é o reconhecimento facial em que o sistema utiliza a imagem facial do usuário para verificar sua identidade durante a autenticação.

4. ESTUDO DE CASO

O estudo de caso hipotético apresentado a seguir, abordará uma empresa do ramo de agronegócio que vem passando pelo processo de transformação digital nos últimos 7 anos. É uma empresa que atua no ramo a mais de 20 anos e por muito

tempo teve seus dados totalmente armazenados fisicamente na sede da empresa, não tendo nenhum tipo de compartilhamento com o mundo exterior.

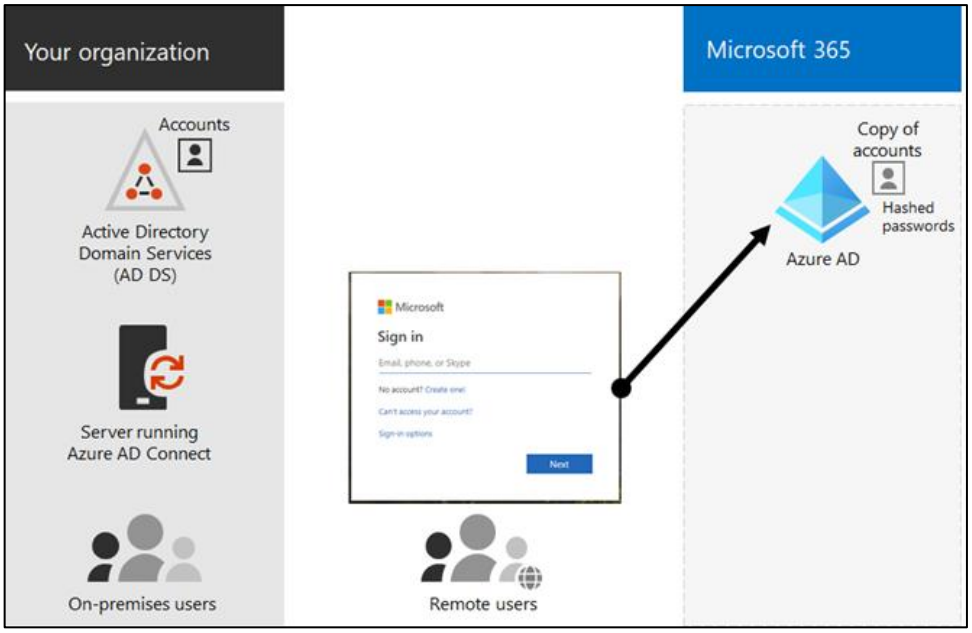
Após perceber que precisa se modernizar para continuar relevante e conseguir ter agilidade em vários processos para atender seus clientes, a AgroForte buscou por soluções tecnológicas que pudessem viabilizar sua evolução. Porém a empresa não poderia e nem era sua pretensão fazer investimentos em equipamentos como servidores e storages, uma vez que esse não é o foco do seu negócio.

Diante desse cenário, a AgroForte encontrou em soluções do tipo SaaS um caminho para se modernizar de forma rápida e com baixo investimento. A AgroForte, possui 2 unidades, nas cidades de Pouso Alegre, MG e Bragança Paulista, SP. A empresa possui 15 funcionários que compartilham uma base de arquivos contendo informações confidenciais de seus clientes, como por exemplo cópia de documentos pessoais, matrículas de imóveis, imposto de renda, fotos dentre outros.

A AgroForte optou pelo uso da solução Office 365 Entreprise, um SaaS da empresa *Microsoft*, cujo modelo de responsabilidade entre cliente e fornecedor está descrito na seção 3.1 deste trabalho. Dessa forma, a empresa fica responsável pelos dados que armazenado na solução, bem como pelos dispositivos e contas de usuários que fazem acesso aos *softwares*.

Cabe ao fornecedor cuidar de todas as aplicações e a infraestrutura para manter a solução disponível 24h por dia. Dentre vários softwares existentes na suíte *Office 365*, a AgroForte faz uso fortemente do *OneDrive* para armazenar e compartilhar dados entre seus funcionários, além de enviar cópias para empresas parceiras quando solicitado.

Imagem 04



Fonte: Microsoft.com. Acesso em: 12/08/2023

Para acessar e compartilhar dados através do *OneDrive*, é necessário fazer a instalação de um *client* em cada notebook ou *smartphone* da empresa. Após a instalação, é necessário efetuar um login com usuário e senha da conta *Office 365*, e cadastrar um fator de MFA para assegurar que a conta só será acessada por pessoas devidamente autorizadas e que contam com uma proteção de segurança em camadas.

Uma vez que a autenticação juntamente com o MFA é executada com sucesso, o dispositivo em questão passa também a ser um dispositivo seguro conectado no *OneDrive*, tornando a partir de então possível o acesso e o compartilhamento de dados da empresa.

Uma vez que o dispositivo está conectado ao *OneDrive*, os funcionários da empresa conseguem ter acesso a 100% dos dados compartilhados internamente pela empresa independente da sua localização geográfica. Aqui vemos o cenário onde os dados podem ser acessados além dos limites físicos da empresa, porém de forma segura e apenas por pessoas com dispositivos que foram previamente autorizados.

Uma conta principal da empresa AgroForte é a conta responsável pelo gerenciamento das demais contas e dispositivos que fazem acesso a seus dados dentro do *OneDrive*. A essa conta, que é de responsabilidade da AgroForte, cabe poderes e responsabilidades para delegar apenas o necessário a quem realmente precisa de acesso.

Essa conta possui plenos poderes para criar novas contas bem como excluir ou restringir contas. Já a cargo do fornecedor, ficam as responsabilidades por manter toda a solução disponível. Isso incluir responsabilidades como adicionar novas funcionalidades a solução, manter os sistemas operacionais seguros e atualizados, além de prover e cuidar da segurança de toda a infraestrutura necessário para manter a solução acessível ao cliente sempre que o mesmo desejar.

5. CONSIDERAÇÕES FINAIS

A segurança informática é um assunto delicado no ponto de vista dos usuários, pois em geral, não gostam de ter a liberdade digital questionada, apresentando dificuldades em lidar com recomendações recebidas, com os cuidados básicos que devem ter, com eventuais restrições impostas, ou mesmo com dificuldade operacionais sugeridas em práticas cotidianas com vistas à segurança em determinadas ações, como enviar um *e-mail*, entrar em uma determinada página da *web*, sacar dinheiro em um caixa eletrônico, fazer transferências, ver fotos de seus amigos em uma rede social, etc.

É a partir dessas situações que a frase "segurança afeta a usabilidade" se tornou popular anos atrás o que parece ser uma afirmação falsa, pois na maioria dos casos, reduzir a inconveniência aos usuários não torna algo mais seguro ou vice-versa e os esforços para eliminar o uso de senhas é um bom exemplo disso.

Os *Speakeasys* usavam senhas para permitir a entrada apenas de pessoas que conheciam a senha. Jogar o jogo de senha era razoavelmente bom enquanto humanos tentavam impedir que outros humanos invadissem os sistemas. A única maneira de entrar no sistema é tentando adivinhar qual é a senha.

O cérebro humano gosta de padrões simples; a senha "12345" é tão fácil de lembrar quanto a palavra "*password*" (ambas são as senhas mais usadas no mundo). As equipes de prevenção decidiram forçar os usuários a usar senhas complexas, iniciando uma corrida armamentista entre os usuários e o pessoal de segurança de TI, situação bem descrita na introdução deste documento.

Então é necessário inventar algo que seja fácil para os humanos e difícil para os computadores. As senhas estão desaparecendo e não apenas para facilitar *logins* ou transações de usuários, mas ao mesmo tempo fornecer uma solução para os principais problemas de segurança atuais.

O *Google* anunciou em agosto de 2019 que o acesso às suas contas e alguns de seus serviços já está disponível por meio de autenticação biométrica ou tela de bloqueio de um *smartphone Android*. Estudos mostram que até 2024 as senhas desaparecerão e com a revisão bibliográfica apresentada no presente trabalho, tal métrica parece ser factível.

REFERÊNCIAS

AMAZON. **Modelo de responsabilidade compartilhada.** 2023. Disponível em: https://aws.amazon.com/pt/compliance/shared-responsibility-model/. Acesso em: 28 de agosto de 2023.

AVAST.COM. **O que é defesa em profundidade?** 2023. Disponível em: https://www.avast.com/pt-br/business/resources/defense-in-depth#pc. Acesso em: 28 de agosto de 2023.

BRASIL. Lei nº 14.063. **Uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos.** Presidência da República, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/lei-n-14.063-de-23-de-setembro-de2020-279185931>. Acesso em: 10 de agosto de 2023.

MELLO, Thiago Braga de Sá, **Autenticação forte em acessos remotos**: Análise comparativa entre soluções com três fatores de autenticação e estudo de caso sobre o B-Unit, Disponível em: https://pantheon.ufrj.br/bitstream/11422/3360/1/TMello.pdf. Acessado em: 26 de novembro de 2022.

MICROSOFT. **Conceitos básicos de segurança, conformidade e identidade da Microsoft:** descrever os conceitos de segurança, conformidade e identidade, disponível em: https://learn.microsoft.com/pt-br/training/paths/describe-concepts-of-security-compliance-identity/. Acesso em: 15 de junho de 2023.

MIRANDA, Heitor Carmássio. **Exoneração e limitação de responsabilidade por violações de dados pessoais nos contratos de computação em nuvem.** 2021. Tese de Doutorado.

RODRIGUES, Anderson da Silva. **O que é autenticação de dois fatores e por que ela é importante**, Diretoria de Gestão de Tecnologia da Informação (DGTI). 2022.

WIKIPÉDIA. **Autenticação**: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Autentica%C3%A7%C3%A3o. Acessado em: 24 de novembro de 2022.