Opinião

Quando uma senha não basta: o desafio de aplicar MFA em todos os acessos

Dennis Brach (*)

O que faz de você quem você é? Sua aparência, suas memórias, suas escolhas, seus relacionamentos? No mundo físico, a identidade é algo profundo e multifacetado. No ambiente digital, tudo isso desaparece.

Para um computador, você não é sua história. Você é um login, uma senha, um cookie de sessão ou um código enviado ao celular. Essa é toda a prova de existência que o sistema reconhece. E se outra pessoa tiver acesso a esses mesmos fragmentos, será tratada como se fosse você.

No mundo online, a identidade não é quem você é, mas o que o sistema aceita como prova da sua existência. É justamente nesse espaço, entre quem você é e o que o sistema reconhece, que os cibercriminosos atuam. Quando conseguem se passar por você, conquistam uma brecha que permite a movimentação em ambientes protegidos e acesso a dados valiosos que alimentam toda uma economia do crime digital.

Por que o MFA é essencial

Muitas pessoas ainda acreditam que identidade digital se resume a um nome de usuário e uma senha. Isso é como trancar a porta de casa com um simples trinco. Pode manter o vento do lado de fora, mas não impede a entrada de um ladrão.

A autenticação multifator, conhecida como MFA, adiciona uma camada extra de proteção ao exigir que o usuário prove sua identidade de mais de uma forma. Esse processo torna muito mais difícil para um invasor acessar um sistema, mesmo que tenha obtido uma das credenciais.

Entendendo os fatores de autenticação

O MFA combina diferentes tipos de provas de identidade:

- Algo que você sabe: uma senha ou um PIN.
- Algo que você tem: um celular, um token físico ou um aplicativo autenticador.
- Algo que você é: uma impressão digital ou reconhecimento facial.

Cada fator pode ser mais ou menos seguro. Um PIN que muda regularmente é melhor do que o mesmo código usado há anos. Uma impressão digital validada por hardware seguro é mais confiável do que um padrão de desbloqueio de tela. Da mesma forma, um token físico é mais seguro do que um código de SMS, que pode ser interceptado se o número for clonado.

Onde o MFA funciona (e onde nem tanto)

Nos smartphones, as opções de autenticação se limitam a senha, PIN ou biometria. O ideal é garantir um código forte e o uso de hardware biométrico seguro. Se o aparelho for roubado, a proteção depende do bloqueio ou apagamento remoto.

Nos computadores, o sistema operacional oferece opções básicas como senha ou autenticação biométrica. A partir daí, é possível adicionar um segundo fator, como um token físico ou aplicativo autenticador. O cenário mais seguro combina senha e segundo fator; o pior é depender apenas de uma senha fraca.

Nas redes Wi-Fi corporativas, o uso de certificados digitais é a forma mais segura, pois vincula o acesso a um dispositivo específico. Já as senhas, embora fáceis de trocar, também são fáceis de capturar em ataques de phishing. O ideal é combinar certificado e autenticação por usuário e senha.

Nos acessos via VPN, as empresas têm mais flexibilidade. É possível configurar o cliente para exigir senha, autenticação por aplicativo e até verificação da integridade do dispositivo antes da conexão. A combinação entre identidade e verificação de conformidade do dispositivo é a mais indicada, enquanto aceitar apenas senha representa o cenário mais vulnerável.

Nos aplicativos em nuvem, há ainda mais possibilidades. Com provedores de identidade adequados, é possível combinar senha, autenticação por push e token físico. O modelo mais seguro inclui senhas fortes, autenticação multifator e verificação de conformidade do dispositivo. Sem MFA, aumentam as chances de ataques de roubo de credenciais ou phishing.

O desafio do MFA em todos os lugares

Pode parecer simples ativar o MFA, mas na prática cada ambiente tem suas limitações. Celulares aceitam apenas um fator na tela de bloqueio. Computadores permitem combinações, mas exigem integração com o sistema. Certificados digitais são poderosos, porém difíceis de revogar. Aplicativos em nuvem oferecem flexibilidade, mas dependem do provedor de identidade adotado.

Por isso, as equipes de TI precisam avaliar cuidadosamente o contexto de cada login, quais fatores estão disponíveis e como agir quando for necessário redefinir ou revogar acessos comprometidos.

Reforçando a segurança do dispositivo

Antes mesmo de permitir o acesso à rede, é essencial validar o estado do dispositivo. Nos celulares, o gerenciamento pode garantir políticas de complexidade de senha, atualização de aplicativos e sistema, além de bloqueio ou limpeza remota em caso de perda.

Nos computadores, políticas de domínio e ferramentas de gerenciamento ajudam a isolar máquinas comprometidas. Em redes corporativas, soluções de controle de acesso podem validar o tráfego e impedir conexões suspeitas. Em VPNs e aplicativos em nuvem, verificações de perfil do navegador e do dispositivo são fundamentais para evitar acessos indevidos.

O próximo passo na autenticação

Os invasores sempre procurarão o elo mais fraco. Se o MFA for inconsistente, eles encontrarão brechas, seja roubando um cookie para burlar a autenticação em nuvem, seja interceptando um código por SMS.

O objetivo não é perfeição, e sim cobertura. Cada login, seja no celular, notebook, rede Wi-Fi, VPN ou aplicativo em nuvem, deve ter pelo menos duas camadas fortes de autenticação. E o time de TI precisa estar preparado para revogar e redefinir rapidamente esses fatores quando necessário.

Aplicar MFA em todos os lugares significa compreender as forças e limitações de cada fator, escolher a combinação mais robusta para cada contexto e eliminar os atalhos que os atacantes estão prontos para explorar.

(*) Country manager da WatchGuard Brasil.

A bolha de IA deve mesmo estourar...

Eduardo Porter é um é um jornalista e escritor especializado em economia, política e sociedade, que passou por veículos como The Wall Street Journal, Bloomberg e The Washington Post – atualmente escreve no The Guardian e mantém uma newsletter no Substack, uma plataforma que permite a escritores, jornalistas e criadores de conteúdo divulgarem seus trabalhos.

Vivaldo José Breternitz (*)

TrueCreatives_CANVA

Recentemente produziu um texto em que traça paralelos entre Corrida do Ouro na Califórnia e a inteligência artificial na atualidade, texto esse acerca do qual vale a pena refletirmos.

A Corrida do Ouro aconteceu entre 1848 e 1855, quando cerca de 300 mil pessoas acorreram à região, vindas até mesmo de lugares tão distantes quanto o Império Otomano. Os garimpeiros massacraram povos indígenas para tomar o ouro de suas terras ao mesmo tempo que impulsionaram as economias de estados vizinhos e até de países distantes, de onde compravam suprimentos.

A Corrida levou a Califórnia, então um território mexicano, a tornar-se um estado americano. Ainda assim, poucos "49ers", como eram chamados os garimpeiros, enriqueceram; quem realmente fez fortuna foram os comerciantes que vendiam comida e equipamentos a eles. Um desses comerciantes, o imigrante bávaro Levi Strauss, que fornecia calças de denim aos garimpeiros que passavam por São Francisco, talvez seja a figura mais lembrada daquela época.

Hoje, a Califórnia vive outra corrida de investimentos. O "pote de ouro" é menos tangível, mas potencialmente muito maior: a Inteligência Artificial. O que essa nova febre deixará em seu rastro talvez molde o futuro da civilização.

A pergunta que todos parecem fazer é: a IA é uma bolha que deve explodir em breve? Muitos acreditam que sim, incluindo Sam Altman, da OpenAI, o Banco da Inglaterra e o próprio Eduardo Porter. Por outro lado, como explicar o preço das ações da Nvidia, que mais do que dobrou entre abril e novembro, sustentado apenas pela esperança de que a IA produza uma superinteligência capaz de fazer tudo o que os humanos fazem, mas melhor.

A Nvidia, como Levi Strauss em seu tempo, ao menos vende algo concreto: chips de computador. Já as valorizações de empresas como OpenAI ou Anthropic estão baseadas sobretudo em expectativas, talvez sonhos.

O grande desafio é confirmarmos se há realmente uma bolha e, se houver, de que tipo. Será daquelas que devastam a economia ao estourar? Deixará algum legado de valor?

As bolhas compartilham uma característica: investidores apaixonados por um sonho. Mas elas se apresentam em diferentes formas. Há menos de 20 anos, vimos a bolha imobiliária americana, quando os preços das casas atingiram alturas estratosféricas e quase derrubaram o sistema financeiro ao desmoronarem. Pouco antes, foi a bolha das "pontocom", quando se descobriu que empresas como Webvan e Pets.com não valiam bilhões apenas por estarem na internet.

> "O grande desafio é confirmarmos se há realmente uma bolha e, se houver, de que tipo. Será daquelas que devastam a economia ao estourar? Deixará algum legado de valor?

Bolhas assolam as finanças globais pelo menos desde o século XVII, quando investidores holandeses se apaixonaram e depois se desencantaram pelas tulipas. No século XVIII, franceses, holandeses e britânicos criaram a bolha do Mar do Sul, embalados pela euforia com novas rotas comerciais no Pacífico. O episódio terminou com o Parlamento britânico aprovando o "Bubble Act", para conter práticas especulativas consideradas perigosas para o comércio e para seus súditos. No século XIX, nos Estados Unidos, houve uma corrida às ações de ferrovias, que gerou prejuízos imensos a cidadãos comuns.

Praticamente toda nova fronteira de investimento gera uma bolha especulativa. Investidores correm para explorar seu potencial, exageram e depois recuam em massa. Assim, a questão mais importante ao avaliar o frenesi atual em torno da IA não é se a bolha vai estourar, mas quando e qual legado deixará. Será que provocará um sistema financeiro debilitado e uma recessão prolongada, como a bolha imobiliária? Ou terá efeito semelhante ao da bolha das "pontocom", cujo estouro gerou uma recessão relativamente branda e, no fim, legou ao mundo a internet moderna?

A ex-economista-chefe do FMI, Gita Gopinath, calculou que um crash equivalente ao da bolha das "pontocom" poderia gerar perdas da ordem de US$ 20 trilhões nos Estados Unidos e outros US$ 15 trilhões no exterior, valores suficientes para abalar fortemente o consumo e gerar uma recessão.

O impacto na economia dependerá, em grande medida, de como essa onda de investimentos em IA está sendo financiada, o que ninguém sabe ao certo. A bolha imobiliária foi alimentada por uma explosão no crédito hipotecário, com bancos fazendo empréstimos cada vez mais arriscados - quando os mutuários não conseguiram pagar, houve a quebra.

A IA pode produzir cenário semelhante. Se IA estiver sendo financiada apenas com o caixa de big techs como Alphabet, Amazon, Microsoft e Meta, o risco é menor - mas o preocupante é que essas empresas vêm recorrendo cada vez mais a empréstimos. Segundo a Bloomberg, o setor de tecnologia fez quase US$ 250 bilhões em dívidas só neste ano, um recorde. Analistas do Morgan Stanley estimam que serão necessários cerca de US$ 1,5 trilhão para bancar data centers e hardware se IA continuar crescendo no rimo atual.

Outro ponto é se a IA que o Vale do Silício está construindo terá durabilidade. As ferrovias sobreviveram às bolhas do século XIX e a internet sobreviveu ao estouro das "pontocom". Mas será que há algo de valor suficiente para justificar a atual euforia? Ferramentas como ChatGPT ou Claude podem elevar a produtividade empresarial, mas não justificam investimentos do porte que vem sendo feitos, como afirmam profissionais do calibre de Yann LeCun, ex-cientista-chefe da Meta e vencedor do Prêmio Turing (o Nobel da computação).

Se esses profissionais estiverem certos, grande parte dos investimentos atuais em IA podem se revelar erros monumentais; talvez a Nvidia e todos nós estejamos prestes a aprender, mais uma vez, que vender jeans e pás não significa necessariamente que há ouro nas colinas.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

News @ TI

ricardosouza@netjen.com.br

TD SYNNEX premiada no AWS Partner Awards 2025

@A TD SYNNEX anunciou que conquistou múltiplos prêmios como Parceiro AWS 2025, tanto em âmbito geográfico quanto global, reconhecendo líderes em todo o mundo que desempenham papéis fundamentais no que toca a contribuir para que seus clientes impulsionem a inovação e criem soluções na Amazon Web Services (AWS). A TD SYNNEX foi escolhida Parceiro Distribuidor do Ano na América do Norte e América Latina, que reconhece distribuidores que contribuíram significativamente para a receita e o número de parceiros AWS em cada região. A empresa também foi homenageada como Parceiro Distribuidor do Ano nas regões EMEA (Europa, Oriente Médio e África) e América Latina, em reconhecimento às suas importantes conquistas no Setor Público. Anunciados durante o evento de Premiação de Parceiros no AWS re:Invent 2025, os Prêmios Geográficos e Globais para Parceiros da AWS reconhecem uma ampla gama de parceiros que se destacaram em especialização, inovação e cooperação ao longo do último ano (https://lac.tdsynnex.com/br/pt-br/).

Parceria entre Positivo Servers & Solutions e Nutanix

@A Positivo Servers & Solutions amplia sua oferta em parceria com a Nutanix, referência mundial em soluções para nuvem híbrida, data centers e modernização de TI. Desde 2015, essa colaboração busca tornar os data centers brasileiros mais eficientes, ao unir hardware nacional com tecnologia internacional para oferecer plataformas mais seguras, estáveis e escaláveis. De acordo com Marcelo Henrique Schunck, diretor de Soluções de Transformação Digital da Positivo Tecnologia, a parceria com a Nutanix reflete a visão de futuro da empresa. "A Nutanix transformou o mercado ao integrar computação, armazenamento e rede em um único sistema, elevando a eficiência dos data centers. Já produzimos os servidores da americana Supermicro, desde 2008, o que abriu caminho para fabricarmos localmente os appliances da Nutanix. Com tecnologia de ponta e em conformidade com o Processo Produtivo Básico (PPB), já entregamos mais de 5 mil unidades no Brasil, impulsionando a transformação digital em instituições públicas e privadas", afirma (https://www.positivoservers.com.br/) (https://www.nutanix.com/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.