Identidade digital é o novo escudo das empresas

O mais recente ataque ao sistema financeiro brasileiro se tornou um caso emblemático sobre como o conceito tradicional de perímetro corporativo ficou ultrapassado

Felipe Guimarães (*)

Com criminosos explorando identidades legítimas para invadir sistemas, fica claro que proteger acessos e credenciais tornou-se o principal desafio das organizações. Em vez de mirar exclusivamente na infraestrutura técnica, cibercriminosos agora se concentram no fator humano, utilizando credenciais válidas para acessar informações confidenciais sem levantar suspeitas.

vege_CANVA

No último grande ataque registrado no país, invasores utilizaram contas legítimas roubadas para distribuir malwares de forma silenciosa, expondo vulnerabilidades graves na gestão de identidade das empresas envolvidas. Ataques baseados em credenciais roubadas já representam mais de 70% dos incidentes cibernéticos globais, com perdas anuais que chegam a US$ 13 milhões por empresa. Na América Latina, essa realidade é ainda mais crítica, com 82% das violações decorrendo justamente do mau uso de credenciais ou falhas humanas.

Identidade digital: o novo perímetro de segurança - A aceleração da transformação digital trouxe não apenas agilidade e inovação aos negócios, mas também desafios complexos para a segurança corporativa. Com o modelo tradicional de proteção baseado em infraestrutura ficando obsoleto, o perímetro físico das organizações, antes facilmente demarcado por redes internas e firewalls, perdeu sua relevância.

Atualmente, o conceito de perímetro é fluido, moldado pelo comportamento dinâmico dos usuários e pela forma descentralizada com que os sistemas são acessados. Nesse contexto, a identidade digital é, agora, a nova fronteira crítica, impondo uma mudança estratégica profunda: as empresas precisam garantir que cada credencial, cada usuário e cada dispositivo sejam continuamente verificados e validados antes de acessar informações sensíveis ou executar transações críticas.

Essa nova dinâmica de segurança está alinhada à filosofia do modelo Zero Trust, cuja premissa básica é nunca confiar implicitamente, independente do ponto de acesso. O perímetro agora é formado pela própria identidade dos usuários e dispositivos autorizados, redefinindo o que se entende por segurança eficaz.

Diferentemente da abordagem anterior, em que bastava manter o criminoso fora da rede, hoje é fundamental assegurar continuamente que um usuário autorizado não seja, na verdade, um invasor disfarçado. O conceito central é a autenticação permanente e adaptativa, em que cada requisição de acesso passa por múltiplas camadas de verificação contextual, incluindo análise de localização, dispositivo, comportamento e horário, além da identidade propriamente dita.

Gestão de identidades: ponto nevrálgico para cibersegurança - A gestão inadequada de identidades digitais abre espaço para ameaças críticas como movimento lateral, quando invasores usam uma única credencial comprometida para acessar diversos sistemas internos, explorando permissões excessivas.

Além disso, falhas simples, como a dependência exclusiva de senhas fracas, permitem acesso indevido, possibilitando que atacantes se disfarcem de usuários legítimos para obter dados confidenciais sem serem detectados. Fraudes internas, realizadas por usuários mal-intencionados ou invasores que assumem contas privilegiadas, também se tornam frequentes sem controles rígidos e monitoramento contínuo.

Outra ameaça crescente é o spear phishing, um ataque direcionado que utiliza informações detalhadas sobre executivos ou administradores para criar comunicações altamente convincentes, induzindo as vítimas a entregarem suas credenciais ou acessos privilegiados.

Por fim, substituir senhas estáticas por métodos mais robustos, como passkeys baseadas no padrão FIDO ou autenticação por certificados digitais, reduz significativamente o risco associado a credenciais vulneráveis ou repetidas. Na prática, empresas que adotaram esses mecanismos enfrentaram menos tentativas de fraude, comprovando que uma estratégia sólida e contínua de proteção de identidades é fundamental para blindar organizações contra o atual panorama de ameaças digitais.

Diante desse cenário, as empresas precisam adotar algumas medidas de proteção, tais como: uma forte governança de identidades, com políticas claras para gestão de IAM (Identity and Access Management), e segmentação de redes e aplicações, com controles reforçados para acessos críticos, como autenticação multifator, ajuda a limitar danos em caso de invasão, bloqueando movimentos laterais e protegendo áreas mais sensíveis.

Além disso, o uso da Inteligência Artificial (IA) para monitoramento contínuo e análise comportamental em tempo real pode trazer uma camada extra de monitoramento ao perímetro. Por fim, é fundamental consolidar uma cultura corporativa de segurança por meio de treinamentos regulares e simulações práticas, garantindo que todos – do nível operacional à alta gestão – estejam preparados e conscientes de seu papel na prevenção de ataques baseados em roubo ou manipulação de identidades digitais.

Em um momento no qual a ameaça é dinâmica e o perímetro de segurança está pulverizado em milhares de identidades digitais, a defesa corporativa precisa evoluir constantemente. Proteger a identidade não significa apenas adotar tecnologias avançadas, mas implementar uma estratégia completa que envolva governança rigorosa, conscientização contínua e uso inteligente de recursos como IA e autenticação adaptativa.

(*) CISO da Solo Iron.

A nova arquitetura regulatória do Banco Central

Maísa Amaral (*)

Os ataques recentes ao sistema financeiro brasileiro não foram um incidente isolado

Eles expõem um vetor cada vez mais relevante: a borda do sistema, onde prestadoras de serviço de tecnologia (PSTIs) e instituições de pagamento ainda não autorizadas vinham se conectando ao Sistema Financeiro Nacional (SFN) sem o mesmo nível de supervisão prudencial que bancos e IPs autorizadas. A decisão do Banco Central de reconfigurar esse perímetro de risco é mais do que uma reação, é uma mudança estrutural na forma de pensar segurança e resiliência.

Entre as medidas anunciadas, o teto de R$ 15 mil por operação para determinadas instituições funciona como um rate-limit regulatório, ou seja, reduz o raio de explosão de um ataque e aumenta o custo operacional para agentes maliciosos. A curto prazo, tesourarias que operam fluxos acima desse valor precisarão fatiar transações e rever janelas de liquidez, mas o impacto sistêmico é limitado, já que mais de 99% das operações PJ estão abaixo desse patamar. O ganho está em observabilidade, permitindo que volumes anômalos apareçam como padrões repetitivos e sejam detectados antes de gerar perdas massivas.

O Banco Central também impôs capital mínimo de R$ 15 milhões e ampliou requisitos de governança, risco e continuidade para PSTIs. Essa mudança é crucial: quem conecta instituições ao SFN passa a ser reconhecido formalmente como infraestrutura crítica, com a responsabilidade de absorver perdas, garantir SLAs e operar com planos robustos de contingência. Em outras palavras, não basta oferecer tecnologia; é preciso demonstrar resiliência compatível com o papel sistêmico desempenhado.

Pix: clareza de responsabilidades

Outra medida de destaque é a restrição de quem pode ser responsável Pix por instituições não autorizadas, limitando esse papel a segmentos S1–S4 (não cooperativas) e estabelecendo prazo de 180 dias para adequação contratual. Isso fecha uma brecha que criava responsabilidades difusas e permitia fragilidades em pontos de autenticação e autorização. Na prática, é uma forma de endurecer fronteiras e clarificar ownership do risco operacional.

É importante ressaltar que a infraestrutura central do Pix permaneceu íntegra. Assim, os prejuízos ocorreram em contas-reserva de instituições que utilizavam prestadores externos e isso reforça um ponto essencial de engenharia: precisamos aplicar uma mentalidade de segurança perimetral rígida, autenticação forte, segregação de ambientes, rotação de chaves e mecanismos de contenção transacional. Isso tudo não apenas no núcleo, mas também nas conexões periféricas que compõem o ecossistema.

Uma arquitetura regulatória adaptativa

Mais do que responder a incidentes, o Banco Central está introduzindo uma arquitetura regulatória adaptativa. Autorização prévia, certificação técnica independente e limites condicionais criam um gradiente de confiança: quem comprova controles sólidos ganha autonomia; quem não, opera sob restrição. O recado é claro: inovação continua bem-vinda, mas precisa ser acompanhada de resiliência mensurável.

Portanto, o Brasil segue como referência mundial em infraestrutura de pagamentos. A lição desse episódio é que a sofisticação dos ataques evolui com a sofisticação dos sistemas. A decisão do Banco Central não somente mitiga riscos imediatos, mas sinaliza um novo patamar de maturidade regulatória, o qual combina segurança, inovação e confiança. Para instituições, fintechs e PSTIs, o desafio agora é alinhar engenharia e governança para estar à altura dessa nova realidade.

(*) Co-fundadora e Chief Legal Officer da Lerian.

Edital de Intimação prazo de 20 dias. Processo Nº 0026436-24.2022.8.26.0002 O MM. Juiz de Direito da 13ª VC, do Foro Regional II - Santo Amaro, Estado de SP, Dr. Caio Moscariello Rodrigues, na forma da Lei, etc. Faz Saber a **Marisa de Paula**, CPF 091.000.038-75 e seu cônjuge **ECKART FARR** (CPF desconhecido) que lhes foi proposta uma ação de Cumprimento de sentença por parte de **Momentum Empreendimentos Imobiliários Ltda**. No bojo desses autos, foi deferida a penhora do imóvel descrito na matrícula nº 50.464 do Cartório de Registro de Imóveis e Anexos da Comarca de Avaré - SP em nome dos réus, tendo sido nomeada como fiel depositária a ré Marisa. Encontrando-se os réus em lugar incerto e não sabido, foi determinada a sua Intimação, por Edital, sobre tal penhora. Transcorrido o prazo deste edital, os réus terão o prazo de 15 dias úteis para apresentar impugnação. Será o presente edital, por extrato, afixado e publicado na forma da lei. Nada Mais. Dado e passado nesta cidade de SP, aos 05/09/2025.

PROTOCOLO DE ASSINATURA(S)

O documento acima foi proposto para assinatura digital na plataforma Certisign Assinaturas. Para verificar as assinaturas clique no link: https://assinaturas.certisign.com.br/Verificar/33F4-3DCC-5F52-41B9 ou vá até o site https://assinaturas.certisign.com.br:443 e utilize o código abaixo para verificar se este documento é válido.

Código para verificação: 33F4-3DCC-5F52-41B9

Hash do Documento

75443010DA40E08FCC742C27A857B2A0DF641BB83B63C1C07D3C000E5F05B21D

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 16/09/2025 é(são) :

☑ Lilian Regina Mancuso - 05.687.343/0001-90 em 16/09/2025 19:42 UTC-03:00
Tipo: Certificado Digital - JORNAL EMPRESAS E NEGOCIOS LTDA - 05.687.343/0001-90