INOVAÇÃO EM DESTAQUE

Inovação: uma arma importante na luta contra os demônios cibernéticos

A inovação, a informação e a cooperação fortalecem as defesas contra os cibercriminosos.

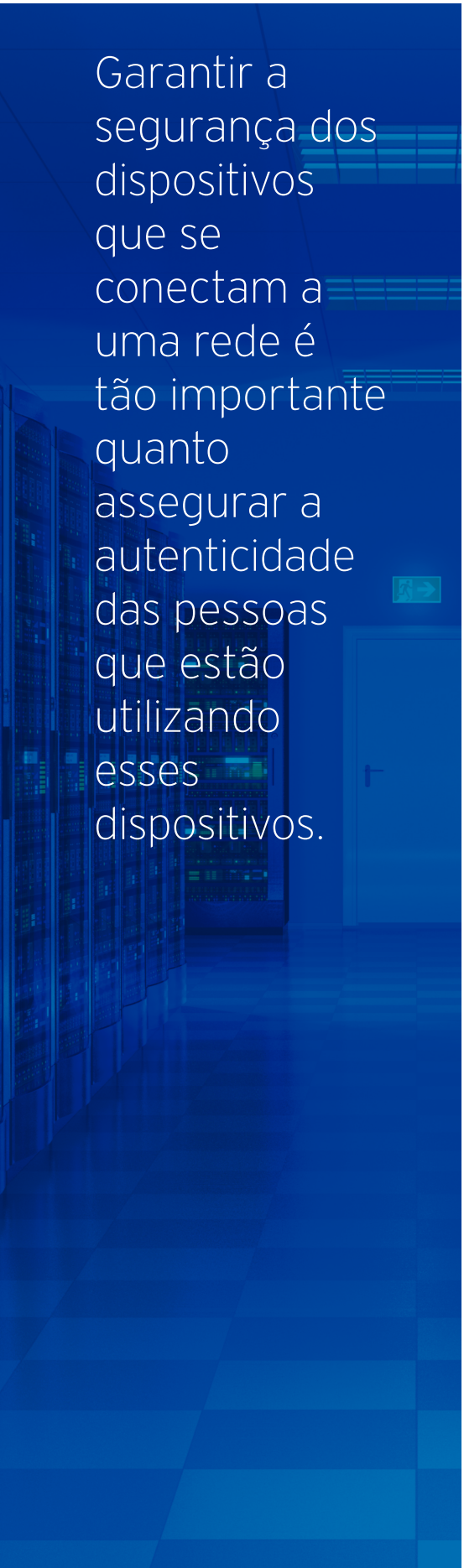
Rajesh Shenoy
Gerente Global de Produtos, Segurança Digital, Treasury and Trade Solutions, Citi

Os bancos e as empresas sempre foram alvos de ladrões, trapaceiros e caloteiros. Os dias dos roubos de ônibus, no entanto, ficaram no passado. Mesmo as caixas registradoras e os cofres cheios de dinheiro que atraíram criminosos durante séculos poderiam se tornar algo do passado à medida em que os consumidores e as empresas migram para os pagamentos virtuais.

Hoje em dia os ladrões e os hackers percebem que a digitalização é mais conveniente. Estão causando cada vez mais estragos financeiros no mundo cibernético, não no mundo físico. De fato, os crimes cibernéticos passaram a ser muito frequentes em todo o mundo. De acordo com um estudo da Juniper Research, o custo desse tipo de delito para a economia mundial será de 2,5 trilhões de dólares no ano de 2019.

Nos Estados Unidos, a preocupação com a continuidade dos crimes cibernéticos fez com que criassem o Centro de Integração de Inteligência de Ameaças Cibernéticas para acelerar as defesas das Agências Governamentais contra os ataques cibernéticos.

Da mesma forma, os governos e as empresas de todo o mundo travaram uma guerra absoluta contra os cibercriminosos. Os bancos têm incrementado sua estratégia no campo de batalha com inovações baseadas em tecnologia que reforçam não só sua capacidade, mas também a de seus clientes, no sentido de ajudar a detectar e evitar um crime cibernético.



Um Monstro com Vários Tentáculos

As ameaças cibernéticas surgem de múltiplas fontes dentro e fora de uma organização, e seus tentáculos podem ser de grande alcance. Tome como exemplo o ataque em massa à informática de uma empresa multinacional de eletrônica e de mídia. Outro caso crítico, um hacker conseguiu transferir milhões de dólares de uma conta bancária corporativa. As fraquezas operacionais e de segurança podem ter um enorme impacto nas cadeias de abastecimento e nas contas financeiras.

Com tantas atividades financeiras sensíveis, que são automatizadas e digitalizadas, a segurança cibernética é claramente uma prioridade entre as corporações e as instituições financeiras.

As parcerias entre os bancos e seus clientes são críticas para a segurança de ponta a ponta. Os criminosos buscam oportunidades para explorar os elos frágeis e reutilizar os métodos de ataque bem sucedidos continuamente. Alinhar-se e compartilhar informações sobre ameaças e práticas recomendadas de segurança pode reduzir vulnerabilidades, ajudando a proteger todos os sócios e seus ativos.

Enfrentando o Inimigo

Em qualquer batalha, um dos melhores ataques é uma boa defesa. A prevenção, detecção e resposta rápida aos ataques digitais se estendem além da tecnologia, incluindo pessoas e processos. É por isso que as instituições financeiras investiram grande quantia de dinheiro e recursos para criar "fortes cibernéticos" com múltiplas camadas de proteção para suas redes e para os dados que são trafegados por elas. Algumas das armas nos arsenais de segurança dos bancos são visíveis para seus clientes e outras são não, trabalham nos bastidores e só aparecem quando há sinais de brechas ou ameaças.

Existem inovações que ainda não entraram em cena na guerra contra os ciberataques e fraudes. As tecnologias emergentes são analisadas, desenvolvidas e testadas continuamente em centros de Pesquisa e Desenvolvimento, como nos Laboratórios de Inovação do Citi, para assegurar que cumpram com os rigorosos requisitos de segurança e regulamentação e também para melhorar as experiências dos clientes ao acessar e utilizar os serviços bancários eletrônicos.

Autenticações biométricas

As tecnologias de biometria que analisam características físicas ou de comportamento únicas oferecem, por exemplo, possibilidades para otimizar a autenticação do usuário e a verificação de sua identidade. Passam a entrar em cena características de uma pessoa real em vez de algo que elas devem recordar ou levar consigo.

As ferramentas biométricas que os laboratórios do Citi continuam monitorando e testando incluem características físicas como a voz, o rosto, a íris e as tecnologias de impressões digitais. O software especializado utiliza as características naturais e únicas dos clientes para verificar suas identidades. Espera-se que essas tecnologias proporcionem aos clientes, alternativas convenientes à segurança baseada em tokens que utilizam PIN, senhas e perguntas de desafio. Por mais promissoras que sejam as novas tecnologias que estão sendo desenvolvidas, os bancos devem se assegurar que elas cumpram com os maiores obstáculos de segurança antes de habilitar seu uso. Além disso, a proteção de dados biométricos se torna crítica já que é mais fácil reestabelecer uma senha que mudar a biometria de uma pessoa.

Os especialistas em tecnologia bancária também estão avaliando as tecnologias biométricas que podem funcionar como ferramentas passivas para iniciar uma sessão (Fazer login). Estas tecnologias utilizam padrões de comportamento tais como escrever ritmos e movimentos do mouse que são únicos de cada pessoa para determinar se a pessoa que está usando um aplicativo realmente é a correta, e bloquear os imitadores.

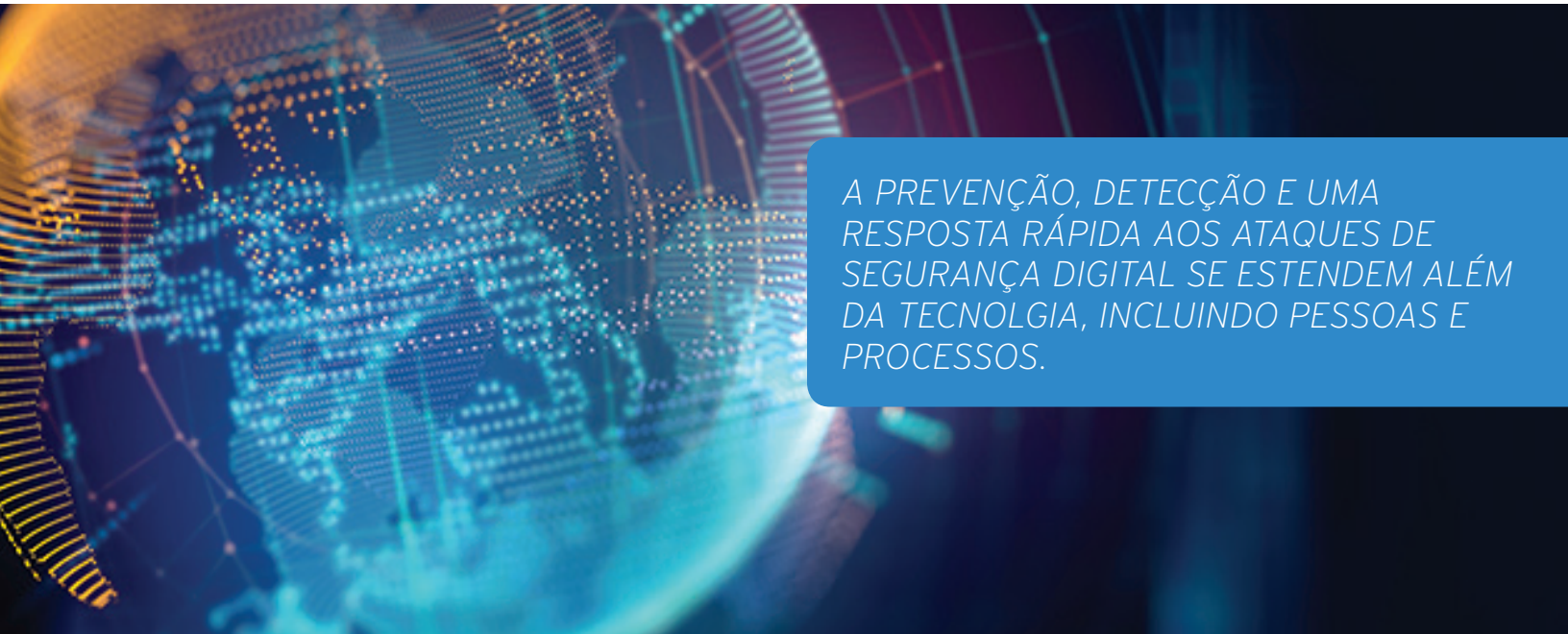
Segurança dos Dispositivos

Garantir a segurança dos dispositivos que se conectam a uma rede é tão importante quanto assegurar a autenticidade das pessoas que estão utilizando tais dispositivos.

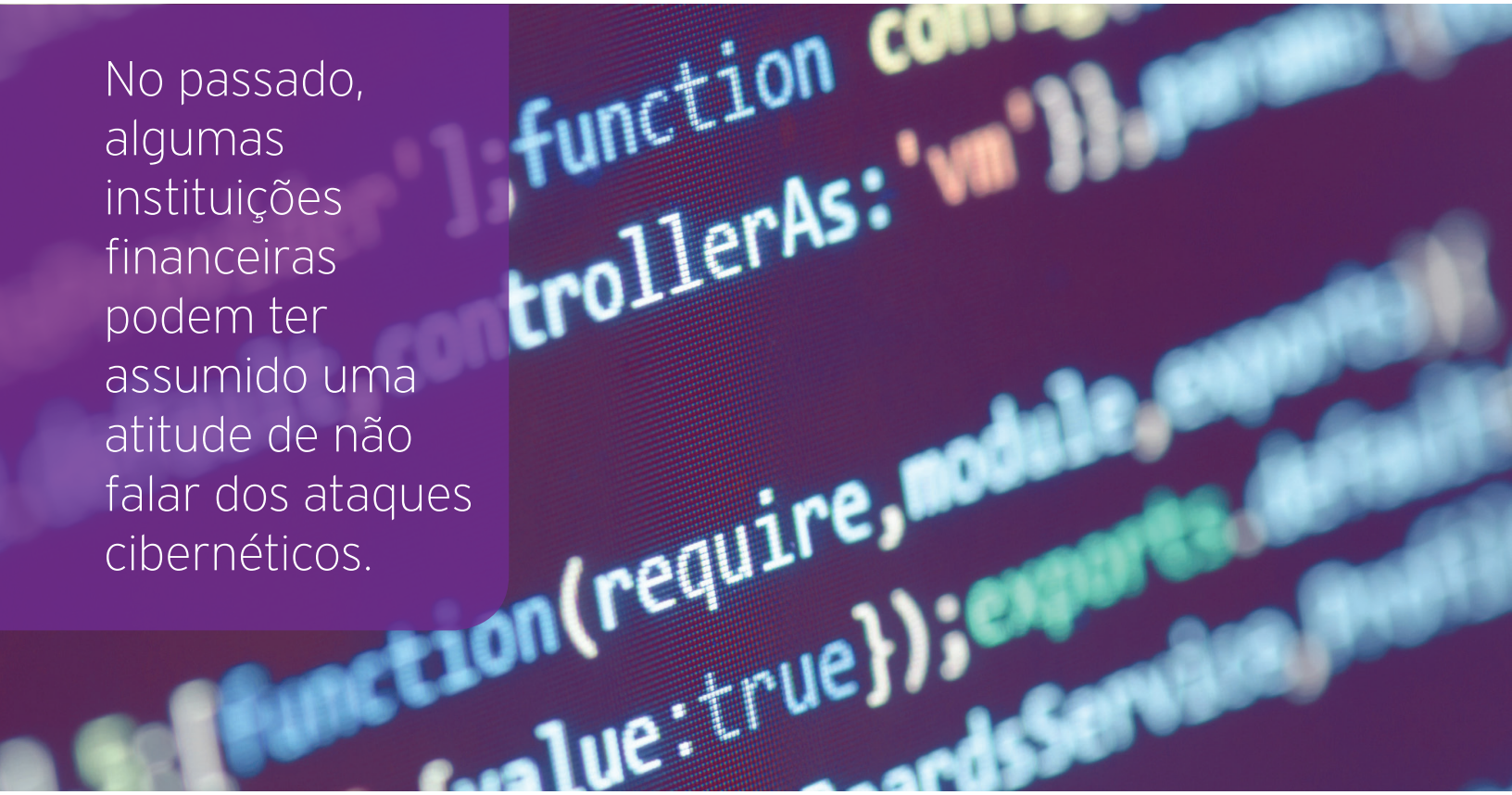
A verdade é que a maior parte da segurança digital se reduz à disciplina e à vigilância por parte dos departamentos de IT e dos usuários finais. O uso de antivírus, a atualização de navegadores e de sistemas, devem ser medidas preventivas periódicas que se estendam aos computadores pessoais e dispositivos móveis que os empregados utilizam para acessar as plataformas da empresa ou para executar transações. Infelizmente, muitos usuários aprenderam em circunstâncias desfavoráveis que o uso de um dispositivo sem proteção, inclusive uma única vez, pode abrir a porta aos criminosos.

Apesar disso, nem todas as empresas e seus empregados são tão cuidadosos no sentido de garantir que as mais recentes proteções contra vírus e malware estejam instaladas e ativas. Os bancos estão tomando consciência das brechas de segurança dos dispositivos de seus clientes e estão aumentando suas defesas para incluir uma nova geração de ferramentas para detectar vírus e malwares. Trata-se de softwares que são inseridos na rede interna do banco e proporcionam verificações de integridade nos dispositivos externos conectados ao banco, buscando sinais de modificação maliciosa ou de infecção.

A evolução das tecnologias de segurança dos dispositivos e a consolidação das informações digitais pelos bancos permitem monitorar as credenciais dos clientes que estão sendo distribuídas publicamente pelos criminosos, quando cometem uma violação com os dados.



A PREVENÇÃO, DETECÇÃO E UMA RESPOSTA RÁPIDA AOS ATAQUES DE SEGURANÇA DIGITAL SE ESTENDEM ALÉM DA TECNOLGIA, INCLUINDO PESSOAS E PROCESSOS.



Segurança Fora da Banda

Os ladrões cibernéticos estão focados principalmente nas transações e no desvio de fundos para si mesmos. Portanto, a segurança das transações é outro grande pilar da defesa. A priorização nos direitos, incluindo a manutenção e atualização dos privilégios, e o uso de múltiplos níveis de autorização são ótimas medidas para garantir que a pessoa correta está iniciando e executando transações, mitigando as possibilidades de que um empregado desonesto interceda maliciosamente nos processos de uma transação.

Ter um conjunto diversificado de pessoas e processos envolvidos em transações de alto valor aumenta o controle e pode reduzir a possibilidade de fraude. Com tal fim, as autenticações fora da banda são outra forma que os bancos estão pesquisando para adicionar uma camada extra de segurança no nível das transações.

As interações fora da banda implicam no uso de um dispositivo separado do canal bancário primário para exigir um nível adicional de aprovação ou confirmação da transação. Em um exemplo de segurança fora da banda de baixa tecnologia, quando uma companhia de cartões de crédito envia por correio um novo cartão a um titular, este deve ligar para um número 0800 para ativá-lo. Em um exemplo de tecnologia superior para uma transação de Internet Banking, um pagamento de alto valor ou transferência de fundos iniciada on-line poderia ser autenticado mediante uma senha única enviada ou uma ligação realizada ao dispositivo móvel do usuário para ter um nível adicional de segurança.

O uso extensivo de dispositivos móveis entre os gerentes corporativos fomentou novos modelos para a segurança digital, assim como as oportunidades de fazer com que o internet banking seja mais conveniente. O Citi, por exemplo, lançou para clientes corporativos que utilizam o Internet Banking Corporativo uma versão de aplicativo para tokens de segurança que simplifica o processo de login na plataforma CitiDirect BE. O novo aplicativo de token pode eliminar a necessidade de que os usuários sejam portadores de tokens físicos para se conectarem de forma segura à plataforma. Em vez disso, podem utilizar o aplicativo em seus smartphones para gerar senhas dinâmicas e se conectar ao CitiDirect BE. O Citi também está lançando, como piloto, o uso de SMS e Código por voz como uma alternativa aos tokens físicos para fazer login nas versões do CitiDirect BE para celulares e tablets com o fim de ver saldos e autorizar transações bancárias.

Mitigar os Riscos dos Pagamentos por meio de Análises

Os especialistas em tecnologia também estão buscando usar ferramentas analíticas de dados para identificar transações de pagamento incomuns e potencialmente fraudulentas. O aproveitamento de grandes volumes de dados de pagamentos entre países, moedas, métodos de pagamento, beneficiários, etc. cria uma linha de base dos padrões normais de atividade dos pagamentos. Usando esses dados, os cientistas de dados do Citi estão explorando modelos estatísticos para monitorar as transações e alertar os clientes quando elas diferirem das tendências históricas. Se, por exemplo, houver uma mudança no padrão de pagamentos recorrentes a um beneficiário, ou se os pagamentos forem feitos a um país diferente do usual, ou se os pagamentos forem autorizados por alguém que não seja a pessoa normalmente autorizada, os alertas podem ser disparados.

Uma Cruzada Compartilhada

A missão é prevenir, detectar e responder à fraude e ao roubo de dados. As "experimentações inteligentes" contínuas dos Laboratórios de Inovação do Citi desenvolvem novas soluções, aproveitando as tecnologias emergentes. Nos proporcionando uma série de novas capacidades que têm nos permitido estar seguros das ameaças emergentes.

No passado, algumas instituições financeiras podem ter adotado uma atitude de "não falar" sobre os ataques cibernéticos. Atualmente, já não é assim. Dadas as altas implicações, as entidades financeiras e seus clientes devem trabalhar juntos e se comunicarem de maneira rápida e eficiente sempre que for detectada uma brecha de segurança. Uma das razões é que quanto mais prontamente todas as partes e autoridades souberem de uma intrusão cibernética, mais provável é que o culpado possa ser preso e que os fundos roubados possam ser recuperados.

A segurança é mais do que proteger os sistemas e recursos. Trata-se de proporcionar tranquilidade, permitindo que as empresas operem sem temor. A inovação e a colaboração são armas de valor incalculável para elevar os ataques contra o crime digital com a maior força possível. Empresas, provedores de serviços bancários, empresas tecnológicas e agências governamentais, tanto no âmbito nacional quanto global, devem permanecer unidas em seus esforços e focadas nas novas opções e inovações de segurança. Compartilhar informação, novas ideias, métodos e melhores práticas entre todas as partes faz com que sejamos todos mais fortes. ■

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions

1575420 07/17