O mercado ancora ameaças fraudulentas em três pilares para priorizar dados e proteger os ativos de uma empresa: a combinação de tecnologias de ponta, estar ciente de potenciais ameaças e punição com penas mais duras contra os crimes cibernéticos

Por Carlos Vieira*

O cenário dos negócios e serviços cada vez mais conectado, ocasionado pela transformação digital e avanço da digitalização no Brasil, mostra às empresas a necessidade de discutir constantemente formas de prevenção de riscos, de estratégias eficazes contra ataques e de proteção para fortalecer a segurança cibernética. O Brasil é considerado um dos mercados mais complexos em relação à prevenção à fraude, mas também é um dos mais avançados e uma referência em inovações e em tecnologias para a cibersegurança.

O crescimento das fraudes digitais no país cresceu estratosfericamente, de acordo com o levantamento global sobre Tendências de Fraude Digital Omnichannel realizado pela TransUnion em 2023: as tentativas de fraude digital aumentaram 80% globalmente desde 2019.

O panorama de ataques no Brasil se arrasta desde os anos 2000, quando em 2002, o phishing tornou-se comum para roubar credenciais de usuários e invadir contas de clientes em instituições financeiras, assim como o surgimento de malwares em 2004. De lá para cá, foram anos da ascensão de RATs (Remote Access Trojans) – inclusive nos dispositivos móveis, das “falsas centrais” com o crescimento de relatos de ataque por meio de sistemas de telefonia, até a transformação digital, com milhões de pessoas entrando no sistema financeiro, sua evolução e o lançamento do Pix, a massificação do uso de Inteligência Artificial em técnicas para burlar autenticação facial, a “laranjização” e a lavagem de dinheiro por meio de Bets.

Para toda essa avalanche de ameaças há mecanismos e tecnologias avançadas de prevenção de riscos para identificar e mitigar vulnerabilidades e proteger transações para evitar a manipulação de consumidores.

Mas, a prevenção à fraude precisa de três pilares para que a segurança digital de fato aconteça: **prevenção**, que requer a adoção de tecnologias emergentes para proteções adequadas, como análise em tempo real, análise comportamental de usuários, bloqueio de ligações suspeitas, autenticação adaptativa; **conscientização**, para educação contínua de usuários sobre prevenção e segurança digital, orientação para denúncias de atividades suspeitas, campanhas em mídias sociais, alertas em tempo real durante e jornada e conscientização sem atritos; e **repressão**, para reprimir crimes cibernéticos, denúncias com rapidez, colaboração entre instituições financeiras, implementação de leis rígidas e aplicação e cumprimento da lei.

Além dos três pilares, outras iniciativas buscam combater atos ilícitos. No ano passado, a Resolução Conjunta Nº 6 emitida pelo Banco Central é uma inovação que fez com que o mercado financeiro colaborasse entre si rumo a um sistema avançado e mais robusto de segurança. Adicionalmente, a identificação de contas laranja está evoluindo junto às instituições, que usam de análise comportamental e de conexões financeiras para identificação de padrões de contas suspeitas para definição do perfil de laranjas, além de cooperação e compartilhamento de informações.

Também, a combinação de tecnologias de ponta com estratégias eficazes de prevenção de riscos são fatores importantes para combater essas ameaças. O mercado financeiro está repleto de soluções de prevenção à fraude e lavagem de dinheiro, que garantem a proteção necessária em transações e segurança de operações. Em todo tipo de transação que possa ser processada pelo sistema financeiro, por exemplo, há diversos aspectos que são calculados, como o uso de algoritmos de inteligência artificial, para entregar informações de riscos e ameaças em tempo real e permitir que o cliente tome uma decisão, seja de bloquear ou liberar aquele procedimento.

Outras soluções baseadas em inteligência artificial - e que empregam tecnologia sofisticada -

garantem a integridade de cada transação e incorporam soluções avançadas antifraude e de combate à lavagem de dinheiro – estes dois conceitos estão intimamente relacionados à fraude. É comum no mercado dizer que 99% das fraudes são seguidas por uma atividade ilícita de lavagem de dinheiro.

Ainda, a IA é uma ferramenta poderosa para combater atos fraudulentos, com aplicações que se utilizam massivamente de algoritmos de machine learning para empregar identificação de anomalias transacionais, comportamento e de habitualidade dos usuários, além de redes neurais, deep learning e técnicas para validações gerais.

Nada é 100% seguro, contudo, estar um passo à frente do cibercrime é o que organizações, governos e grupos continuam fazendo, por meio de um processo robusto de sensibilização, identificação e prevenção de atos ilícitos, cooperando entre si e integrando tecnologias com velocidade para um bem maior: uma sociedade mais segura. Tentativas de fraude devem ser denunciadas, para que nenhum amigo, familiar ou nós mesmos sejamos vítimas de algum crime cibernético.

***Carlos Vieira** é Fraud Prevention Manager da Topaz

Fonte: DFreire, em 15.10.2024