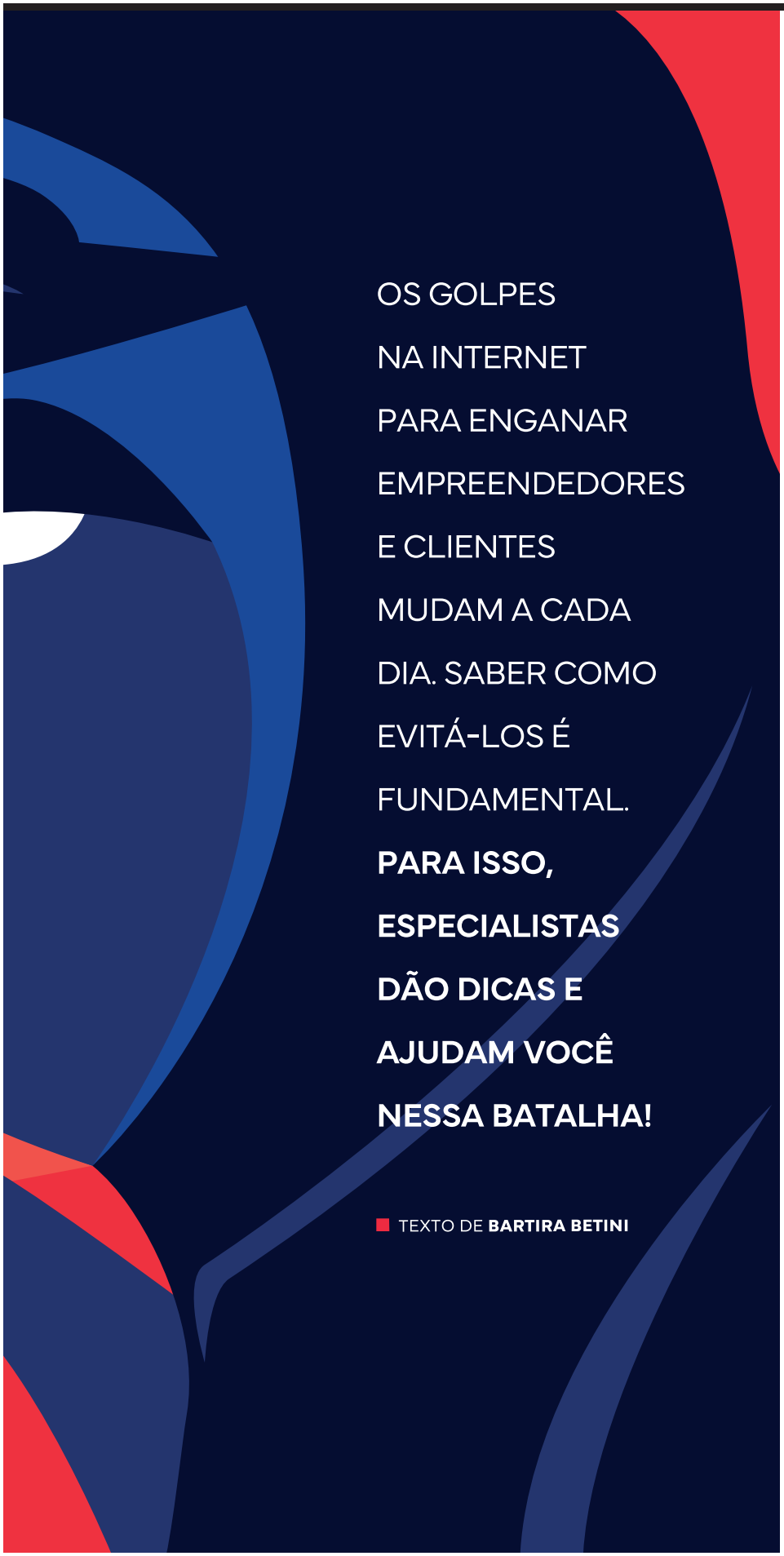
AS FRAUDES MAIS COMUNS NO MUNDO DO E-COMMERCE

OS GOLPES NA INTERNET PARA ENGANAR EMPREENDEDORES E CLIENTES MUDAM A CADA DIA. SABER COMO EVITÁ-LOS É FUNDAMENTAL. **PARA ISSO, ESPECIALISTAS DÃO DICAS E AJUDAM VOCÊ NESSA BATALHA!**

TEXTO DE **BARTIRA BETINI**



© ID-WORK / ISTOCKPHOTO.COM

Uma pesquisa divulgada pela Sophos, empresa britânica de segurança em Tecnologia de Informação (TI), mostrou aumento de 36% no tempo de permanência de cibercriminosos nas redes e nos sistemas invadidos, em uma média de 15 dias em 2021 contra os 11 dias verificados em 2020. O estudo identificou que os cibercriminosos ficam mais tempo em empresas menores, com até 250 funcionários, passando uma média de 51 dias. Já em empresas entre 3 mil e 5 mil funcionários, o tempo médio de invasão é de 20 dias.

Essas empresas pecam quando não encontram o "paciente zero", ou seja, o causador inicial do problema. "Depois que ocorre a invasão, os colaboradores começam a missão de encontrar qual sistema foi atacado, como, onde, que horas, e tentam minimizar o dano removendo a ameaça, mas os ataques seguem aparecendo, porque simplesmente não identificaram o paciente zero. Ao identificá-lo, é possível saber onde o ataque começou, se ele ainda está ativo e quem está mais em risco", explica o perito em crimes digitais e CEO da Enetsec, Wanderson Castilho.

Com mais de 5 mil casos resolvidos, o perito cibernético e físico utiliza estratégias de detecção de mentiras e raciocínio lógico para interpretar os algoritmos dos crimes digitais. Autor de quatro livros importantes no segmento e há 30 anos no mercado, Wanderson Castilho refaz os passos dos criminosos virtuais para desvendar a metodologia empregada no crime digital. Certificado pelo Instituto de Treinamento de Análise de Comportamento (BATI) da Califórnia, responsável por treinar mais de 30 mil agentes policiais, entre os quais, profissionais do FBI, da CIA e da NSA. Também possui certificados em Certified Computing Professional (CCP) – Mastery, Expert in Digital Foren-

sics, é membro da Association of Certified Fraud Examiners (ACFE). E sua recente certificação como especialista em investigação de criptomoedas pelo Blockchain Intelligence Group, ferramenta usada pelo FBI, o coloca hoje em um patamar de um dos maiores profissionais em crimes digitais do mundo, sendo um dos especialistas mais cotados para resolver crimes cibernéticos. "Os cibercriminosos praticam uma tática muito lucrativa, que é manter arquivos digitais de empresas como reféns até que uma taxa de resgate seja paga em moeda virtual, difícil de rastrear", afirma.

O avanço da transformação digital faz com que as empresas se reinventem constantemente, e investir em inteligência é determinante não somente do ponto de vista das vendas, mas também da segurança. Todo o ecossistema envolvido com o e-commerce deve estar atento ao aumento de riscos, o que lhes impõe a dar atenção especial à segurança de aplicações e de dados. "Segurança cibernética deve estar no orçamento das empresas e ser discutida nos conselhos de administração. Esse é o ponto de partida para termos empresas com postura de segurança, com uma cultura em que todos os funcionários saibam que devem se precaver de possíveis ataques", explica o CEO da Agility, Fábio Soto.

© DIVULGAÇÃO / ENETSEX

Depois que ocorre a invasão, os colaboradores começam a missão de encontrar qual sistema foi atacado, como, onde, que horas, e tentam minimizar o dano removendo a ameaça. Mas, **WANDERSON CASTILHO, perito em crimes digitais e CEO da Enetsec,** lembra que os ataques seguem aparecendo enquanto não se identificar o paciente zero: "Somente ao identificá-lo é possível saber onde o ataque começou, se ele ainda está ativo e quem está mais em risco".

Como os ambientes de trabalho estão cada vez mais espalhados, a gestão da segurança dos dados fica mais difícil e a cultura corporativa também se perde um pouco. Isso faz com que existam maiores possibilidades de ataque para os cibercriminosos e maior probabilidade de vulnerabilidades também. Portanto, é importante mudar a cultura de segurança da empresa. Os colaboradores de todos os níveis hierárquicos são responsáveis pela segurança. Essa responsabilidade precisa ser encarada como geral na organização.

As possíveis brechas que abrem os canais para o perigo podem ser, por exemplo, *softwares* desenvolvidos com vulnerabilidades, infraestrutura mal configurada ou mesmo descaso com investimentos relacionados ao tema. Além desses aspectos técnicos, é fundamental que os colaboradores sejam bem treinados e saibam dos riscos ao clicar em um arquivo enviado por e-mail ou por uma rede social. Não se deve descuidar, também, da configuração ou da implementação dos requisitos de segurança para que não aconteça uma invasão. "Por isso, vale apostar em uma boa solução de proteção de nuvem", alerta o especialista da Agility.

POR FALAR EM SEGURANÇA

A segurança do negócio e dos clientes é prioridade para a Privalia, um dos maiores *outlets* do Brasil. Com 17 milhões de pessoas cadastradas e mais de 500 mil visitas por dia, a plataforma de vendas on-line investe permanentemente na busca de soluções antifraude que não prejudiquem a experiência dos usuários.

O CTO da Privalia, Diego Gamboa Olabarri, conta que a estratégia de prevenção a golpes digitais combina tecnologia avançada e um time especializado. "Ter uma pla-

TOME NOTA!

CUIDADOS PARA SUA EMPRESA VENDER NA INTERNET SEM DOR DE CABEÇA

GARANTA DISPONIBILIDADE – A estabilidade do site é fundamental para que a operação funcione plenamente até em períodos de aumento de tráfego, evitando assim que a loja deixe de vender por causa de problemas técnicos. Além do investimento em infraestrutura tecnológica e nas soluções de segurança, é essencial a proteção contra os chamados ataques de negação de serviço (DDoS), que objetivam direcionar volume de acessos simultâneos muito acima do normal para determinado endereço até que ele seja congestionado e fique indisponível.

EXPLORE A WEB – Inclua em seus processos rotinas de *threat intelligence*, ou monitoramento de marca, a fim de pesquisar menções sobre a empresa e seus executivos em fóruns nas diferentes camadas da internet, incluindo a *dark web* e a *deep web*, onde todos os tipos de ataque são encomendados e arquitetados. Com esse tipo de varredura, é possível detectar planos para redirecionamento de tráfego do seu site para páginas falsas da internet ou das redes sociais, evitando dessa forma venda indevida ou fraudulenta de produtos com a sua marca.

CONSCIENTIZE OS COLABORADORES PARA PROTEGER SEUS DADOS – Pesquisas de mercado apontam que as principais portas de entrada para *malwares* utilizados

nos ataques de *phishing* e de *ransomware*, que encriptam os dados em troca de um valor de resgate, são os próprios colaboradores. Na maioria das vezes, por falta de conhecimento, há descuido ao lidar com e-mails suspeitos, conexão de dispositivos USB, acessos a sites comprometidos ou uso de softwares com vulnerabilidades. Com o trabalho remoto, também aumentou o uso de dispositivos pessoais conectados à rede corporativa. Além da tecnologia e dos processos, a conscientização das pessoas é um dos pilares essenciais para garantir a segurança dos dados e não sofrer com a paralisação da operação.

REALIZE BACKUP E VALIDE SUA INTEGRIDADE - Com o objetivo de minimizar os riscos de interrupção dos serviços e garantir que os dados sejam recuperados de forma rápida e fácil, é muito importante ter um sistema de *backup* consistente, testado periodicamente para validação do seu conteúdo e da sua integridade, já que muitos ataques iniciam comprometendo o *backup* e depois impactam o ambiente de produção. Além disso, é imprescindível ter uma documentação com o catálogo de todos os servidores e garantir a ordem de recuperação dos dados em um eventual desastre, reduzindo o tempo de recuperação dos dados.

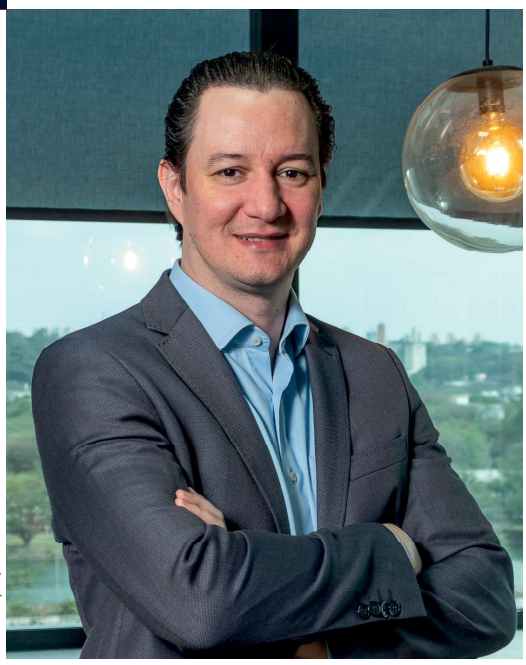
VALIDE SEUS REPOSITÓRIOS DE CÓDIGOS - Uma nova campanha massiva de infecção em lojas de e-commerce está em andamento com o nome de *Hubberstore*. O ataque ocorre a partir de um código JavaScript malicioso, utilizado para extração de dados pessoais e de cartões de crédito.

As recomendações nesse caso são as seguintes:

- Mantenha os sistemas atualizados, incluindo sistemas operacionais, serviços e *frameworks* utilizados nos sites.
- Revise periodicamente os códigos do seu repositório e ambiente de produção, buscando identificar possíveis injeções de artefatos maliciosos.
- Siga as melhores práticas de desenvolvimento seguro. Uma boa referência é o OWASP.
- Analise *logs* e trilhas de auditoria, de preferência utilizando um sistema de correlacionamento de *logs* (SIEM), com o objetivo de identificar tentativas de exploração de vulnerabilidades.
- Implemente uma solução de múltiplo fator de segurança (MFA) nos principais pontos de entrada e em seus principais ambientes de desenvolvimento de código, como repositórios e soluções de CI/CD (integração e entrega contínua).

CONTROLE E LIMITE O ACESSO ÀS INFORMAÇÕES - Garanta que os usuários tenham o mínimo privilégio e restrinja os acessos para as pessoas que realmente precisem, garantindo sua revisão e recertificação periódicas. A implementação de segmentação na rede minimiza o risco de que um ataque se espalhe rapidamente e sem controle, evitando grande impacto e prejuízo financeiro, e, por fim, utilize solução de cofre de senhas para aumentar a segurança nos acessos privilegiados.

Fonte: Eduardo Gonçales, especialista e CISO da TIVIT, multinacional brasileira e *one stop shop* de tecnologia.



© DIVULGAÇÃO / AGILITY

FÁBIO SOTO, CEO da Agility, afirma que a segurança cibernética deve estar no orçamento das empresas e ser discutida nos conselhos de administração: "Esse é o ponto de partida para termos empresas com postura de segurança, com uma cultura em que todos os funcionários saibam que devem se precaver de possíveis ataques".

taforma interna nos ajuda a resolver possíveis violações de maneira mais rápida. Para processos de pagamento acreditamos que a melhor solução é usar ferramentas de terceiros", explica, lembrando que as entidades de pagamento, são obrigadas a cumprir regulamentações internacionais.

Segundo o CTO da Privalia, todo dia surgem novas tentativas de golpe no comércio eletrônico. Como exemplo, cita as chamadas fraudes de teste de cartão, que utilizam dados de cartões de crédito roubados (vendidos na *dark web*) ou gerados por meio de um algoritmo e as compras são enviadas a endereços difíceis de rastrear. "Outra fraude comum é a aquisição de contas, quando os invasores entram na conta do cliente com senhas roubadas ou engenharia reversa e fazem compras, sacam fundos ou acessam outras contas com os mesmos dados", relata.

Entre as principais tentativas de golpe, ele menciona também a fraude de reembolso, quando o invasor compra com um método de pagamento roubado/ilegal e solicita o reembolso usando outro método de pagamento a partir do qual pode

© DIVULGAÇÃO / PLBRASIL

"Vale lembrar que a informação é o bem mais precioso no mundo dos negócios. A falta de segurança de dados pode fazer com que você perca o seu principal ativo: a confiança do seu cliente"

JOÃO GABRIEL FERRARI, ADVOGADO E SÓCIO-GESTOR DO GRUPO PLBRASIL

administrar a quantidade reembolsada; e até fraude de falha na entrega, na qual os clientes alegam não ter recebido a encomenda, e cancelam o pagamento após o envio do produto.

"Para proteger nosso negócio e nossos clientes, adotamos várias medidas antifraude, como a classificação de *whitelisting* e *blacklisting* de clientes, a implementação de autenticação *step-up* e de processos de IA e a *machine learning*, para detectar e bloquear pagamentos fraudulentos", conta Olabarri. A Privalia também utiliza um sistema antifraude, no qual terceiros analisam as transações e os dados de cartão de crédito usados durante a possível fraude. Todos os pagamentos são feitos em um provedor de serviços certificado PCI, com vários algoritmos de validação.

A coordenadora e professora do curso Gestão Estratégica de Franquias do IAG – Escola de Negócios da PUC Rio, Leila Toledo, afirma que uma prática comum no meio digital é o envio de e-mails falsos. Utilizando logo de empresas e, por vezes, até mesmo dados reais do consumidor como isca, golpistas usam desse artifício para obter informações como senhas bancárias, números de cartão de crédito, entre outras. É conhecido como golpe de *phishing*. "Outra forma bastante usual são os golpes pelo WhatsApp. Contas desconhecidas disfarçadas de contas reais entram em contato com o consumidor e enviam *links* para promoções, cupons de desconto. E um dos golpes mais comuns no varejo digital é o roubo de dados. Fraudadores, passando-se por varejistas tradicionais, enviam e-mails ou mensagens pelo celular, oferecendo vantagens. Nesse tipo de golpe, é possível obter dados de consumidores, como CPF, dados bancários, entre outros", pontua.

Existe também o golpe do falso boleto, da conta vencida, que pode ocorrer por e-mail, mensagens do WhatsApp ou SMS. A clonagem de cartões de crédito também acontece no meio virtual, quando os protocolos de segurança do site não estão atualizados. "O varejista deve investir na segurança dos dados e construir uma relação de confiança com o seu consumidor. Garantir um site seguro com certificação é o primeiro passo. Submeter a uma avaliação para exibir selos de segurança são bons recursos. Outra solução é dedicar um espaço na loja virtual para apresentar os protocolos de segurança e informar sobre a política da empresa, como a criptografia dos dados, o não envio de e-mails com anexos, links ou arquivos executáveis."

FRAUDES, AQUI NÃO!

O advogado e sócio-gestor do grupo PLBrasil, João Gabriel Ferrari, dá uma recomendação inicial para quem quer evitar fraudes no e-commerce: "o primeiro passo é procurar um provedor de tecnologia

© DIVULGAÇÃO/ PRIVALIA

"Ter uma plataforma interna nos ajuda a resolver possíveis violações de maneira mais rápida. Para processos de pagamento, acreditamos que a melhor solução é usar ferramentas de terceiros"

DIEGO GAMBOA OLABARRI, CTO DA PRIVALIA

com reconhecimento no mercado quanto a sistemas de segurança para construção do e-commerce, de preferência *players* com certificação na área de segurança da informação e prevenção de fraudes. A tecnologia evolui muito rapidamente e empresas especializadas possuem equipes preparadas e certificadas para desenvolvimento de plataformas robustas para evitar fraudes, invasões e sequestro de dados".

O Grupo PLBrasil tem um comitê de inovação para receber as demandas e apresentá-las aos sócios. Um dos diferenciais da assessoria é o Portal Paralegal, uma plataforma digital de gestão de processos administrativos e de armazenamento de documentos do cliente. "A plataforma tem como foco principal entregar ao cliente o andamento do processo em tempo real, sem que ele precise cobrar *feedback* constante do nosso time. Já pensou se não tivermos segurança digital?", analisa Ferrari e conclui explicando como é necessário estar com todo o controle digital em dia para os clientes e a empresa não sofrer golpes.

O advogado explica ainda que a plataforma deles foi construída com as mais recentes inovações do mercado, inclusive com respeito à Lei Geral de Proteção de Dados ("LGPD"), para evitar fraudes e vazamento de informações e documentos sensíveis de pequenas, médias e grandes empresas. Além da plataforma, adotaram alguns processos internos que visam à rastreabilidade das ações, tais como: solicitar comprovações eficazes de quem utilizará a ferramenta (portal Paralegal) e a adoção do chamado *"background check"*, que consiste em um processo para validação e comprovação de dados, antes da liberação de acesso aos usuários.

João Gabriel Ferrari diz que as empresas precisam se conscientizar cada vez mais da importância e da necessidade corporativa de reforçar a segurança dos seus próprios dados e, principalmente, os de seus clientes. "Além dos enormes prejuízos financeiros que podem ser causados pelo vazamento de informações, a LGPD prevê a aplicação de multas pesadas neste sentido", completa, e ainda ressalta: "vale lembrar que a informação é o bem mais precioso no mundo dos negócios. A falta de segurança de dados pode fazer com que você perca o seu principal ativo: a confiança do seu cliente."

© DIVULGAÇÃO / IAG

Para **LEILA TOLEDO, coordenadora e professora do curso Gestão Estratégica de Franquias do IAG – Escola de Negócios da PUC-Rio**, outra forma bastante usual são os golpes pelo WhatsApp: "Contas desconhecidas disfarçadas de contas reais entram em contato com o consumidor e enviam links para promoções, cupons de desconto. É um dos golpes mais comuns no varejo digital é o roubo de dados".

Fundada em 2009, a Ticket360 é uma startup já consolidada no mercado de show business. Foi idealizada por produtores de shows que entendiam as dificuldades do mercado para a venda de seus eventos e buscavam uma ferramenta na época inexistente que pudesse atendê-los. Comercializando mais de 1.800 eventos anuais, ao longo desses anos a empresa foi identificando diversos desafios no caminho, um desses são as fraudes de cartão de crédito.

Para combater e eliminar esse prejuízo, criou-se um setor antifraude. Inicialmente esse setor era responsável apenas por realizar ligações para os clientes, em um estilo *call center*, para realizar a confirmação de dados do cartão *versus* cliente, solicitando documentos se necessário. Porém, junto com as fraudes que evoluíram, o setor da empresa também cresceu. "Cada vez mais lidamos com fraudadores audaciosos e com golpes muito bem formulados, por isso constantemente estamos investindo em sistemas próprios e externos a fim de diminuir os riscos para nossos produtores de eventos", explica o CEO e fundador da Ticket360, Fabio Salva. Hoje são no mínimo dez funcionários diariamente lidando com os desafios dos golpistas, considerando que pelo menos 3% das tentativas de compras são fraudulentas.

A empresa conta com um sistema próprio desenvolvido internamente que consiste em robôs identificando comportamentos estranhos do usuário e cadastros com informações divergentes, baseados em geolocalização e IP, também utilizam um sistema que capta há quanto tempo aquele e-mail que o cliente está usando existe, além de um sistema próprio com inteligência artificial que gera *tokens* verificando a veracidade dos dados do cartão *versus* a informação enviada pelo banco emissor ao portador do cartão. Ainda assim, com todo esse investimento em tecnologia, também são contratados sistemas externos para auxiliar essas verificações.

"Já nos deparamos com todo tipo de fraude do mercado, fraudadores de cartão sempre fazem testes em ticketeiras para checar se o cartão irá funcionar, por isso nossa preocupação e investimento constante nessa área", ressalta o fundador da empresa. "Além dessa modalidade de autofraude, que é aplicada pelo usuário comum, existem outras diversas, como clonagem de dados do cartão, golpe do depósito bancário, roubo de cartão. Todos os dias aparecem novos golpes e devemos estar preparados para evitá-los", alerta e finaliza Fabio Salva. G&N PME