RELATÓRIO EXCLUSIVO

SEGURANÇA Digital

Setembro **2021**

Empresas e home office

Como priorizar a segurança de dados

momento EDITORIAL

BETC HAVAS

Open Banking as a Service TecBan

Nossa experiência em conectar mais de 150 instituições vai acelerar a entrada da sua empresa no Open Banking.

O Open Banking as a Service TecBan foi desenvolvido para reduzir a complexidade da implantação, os custos e o tempo de execução. Uma solução completa, segura e a única já em operação no Brasil.

A TecBan faz acontecer.

tecban.com.br
linkedin.com/TecBan

TecBan

APRESENTAÇÃO

Estamos trazendo para você esta edição única de 2021 sobre **Segurança Digital**. Com reportagem e produção de textos da jornalista Wanise Ferreira este e-book colhe as opiniões e traz informações sobre o que promete ser o maior desafio para a transformação digital das empresas.

Neste e-book, estão contidas as reflexões sobre os desafios para o Open Finance e os riscos que chegam com os milhões de dispositivos a serem conectados na Internet das Coisas.

Aborda também os recentes sequestros de dados nas redes varejistas brasileiras e a avalanche trazida com a epidemia do covid-19 e a rápida migração para o *home office*.

A segurança digital é e será tema de atenção de toda a qualquer corporação e, por isso, presentamos você, leitor, com esse primeiro relatório.

Boa Leitura!

momento EDITORIAL

Edição
Miriam Aquino

Edição de Arte
Rael Lamarques

Reportagem e Texto Final
Wanise Ferreira

Imagens/Ilustrações
Freepik | Banco de imagens das empresas entrevistadas

Administrativo-Produção
Gerente: Adriana Rodrigues
Produção: Camila Carvalho

Web e Suporte de Rede
Leandro Morais
Ricardo Oliveira

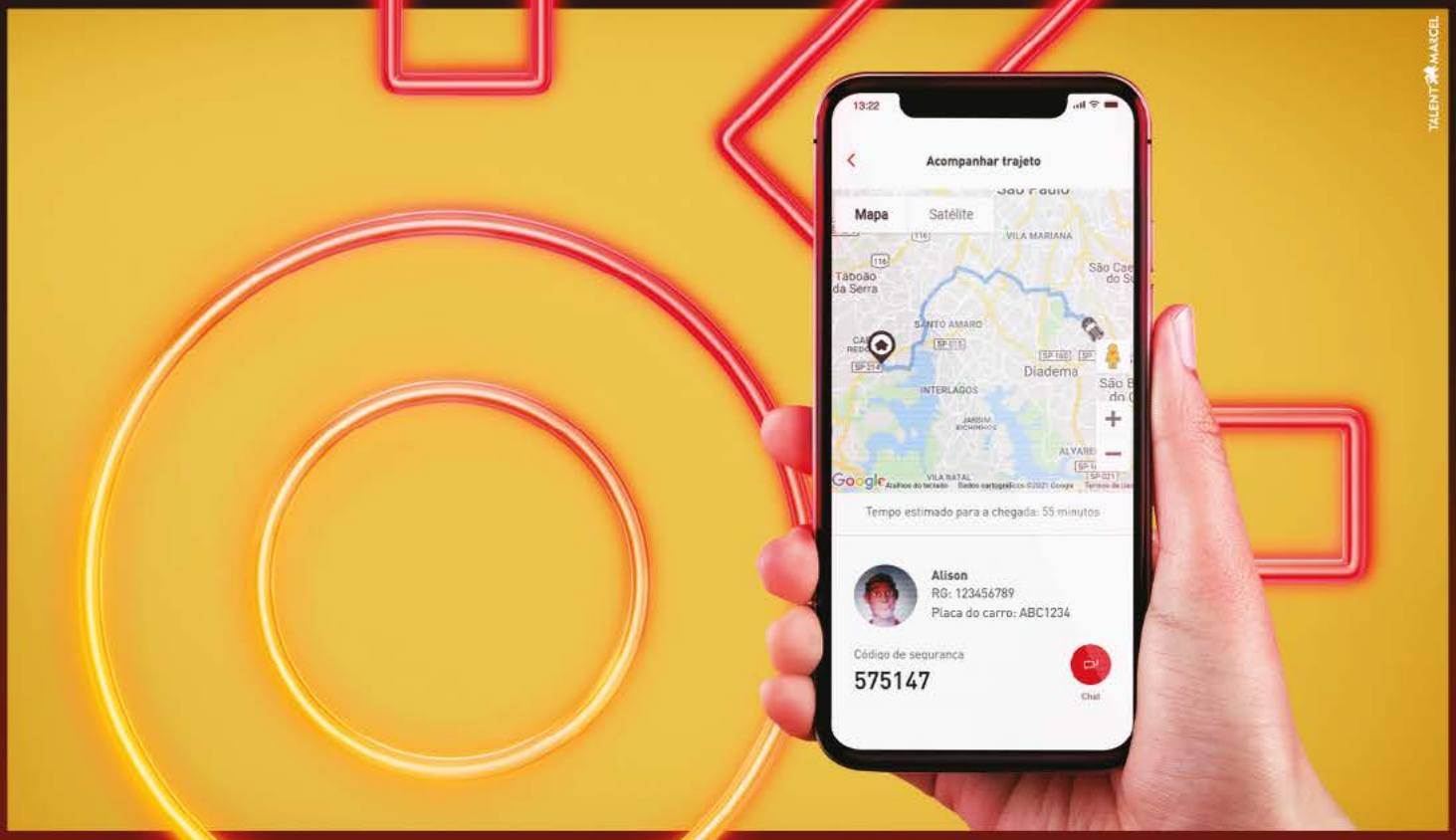
Publicidade
Tarsila Maria Araújo
tarsila@armazemdecomunicacao.com.br

Armazém da Comunicação
(61) 99979-3440
Zélia Maria
zelia@zmcrepresentacoes.com

ZMC Representações
(61) 99986-2467

Jornalista responsável
Miriam Aquino (DRT 3746-DF)

Uma publicação da
Momento Editorial Ltda
Rua São Sebastião, 820 Sala 42E,
Santo Amaro
São Paulo - SP - 04708-001
Fone: 11 - 3124-7444
Celular: 11 - 98372-8558



TALENT MARCEL

TECNOLOGIA COM SEGURANÇA & MUITO MAIS

Segurança é um assunto sério e depende de todos nós. Tentativas de fraude, infelizmente, são uma realidade, mas a Claro, através dos apps Minha Claro, usa inteligência e tecnologia para cuidar da segurança dos seus clientes.

Os apps Minha Claro são canais exclusivos com a Claro e neles, além de ser possível agendar e acompanhar visitas técnicas, o cliente também acessa sua fatura digital com garantia de autenticidade e ainda conta com muitas outras facilidades.

Minha Claro residencial
BAIXE O APP

Minha Claro móvel
BAIXE O APP

Confira mais dicas de segurança em **claro.com.br/seguranca**

Claro

Você merece o novo.

/embratel

Novas oportunidades geram novos riscos. E todos os dias inventamos novas formas de nos proteger, cada vez mais seguras e eficientes. Vamos criar juntos o próximo nível?

Fale com nossos especialistas ou conheça as soluções para sua empresa em embratel.com.br

CONECTIVIDADE MOBILIDADE COLABORAÇÃO SEGURANÇA IOT CUSTOMER EXPERIENCE PROFESSIONAL SERVICES CLOUD DATA CENTER

Embratel
SUA EMPRESA NO PRÓXIMO NÍVEL

O OPEN FINANCE

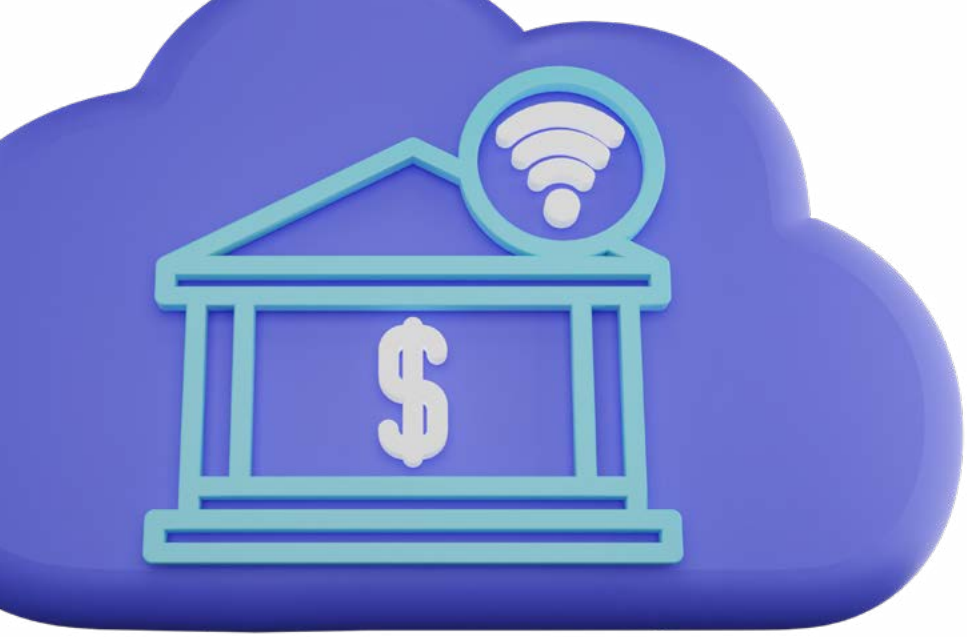
E SEUS DESAFIOS ESTÃO A CAMINHO

A transição começa com o Open Banking e carrega as preocupações com segurança em um ambiente inovador

As instituições financeiras – bancos e *fintechs* – prosseguem atendendo ao cronograma determinado pelo Banco Central para implantação do Open Banking que, em sua última etapa, se torna conceitualmente Open Finance com a adesão de novos *stakeholders* como corretoras, companhias de câmbio, fundos de previdência, seguradoras e outros. A proposta, como está implícito, é um sistema financeiro mais aberto no qual o cliente passa a ser dono de seus dados e de suas escolhas e permite que determinadas informações possam ser compartilhadas dentro de um mesmo ecossistema.

A partir dessas inovações, se espera mais competição, criação de novos serviços e aumento no volume de negócios. Mas é muito importante ressaltar que quando estão juntas as palavras "aberto" e "sistema financeiro" há uma imediata e constante tensão no que diz respeito à segurança de dados, e é no esforço de proteção de eventos que todos os envolvidos nesses processos estão – ou pelo menos, deveriam estar – se dedicando.

A primeira fase do Open Banking, de acordo com o BC, já foi concluída com o compartilhamento de informações das próprias instituições, como canal de atendimento, produtos e serviços. A segunda fase – inicialmente prevista para 15 de julho mas adiada para 13 de agosto – envolve a autorização do cliente para o compartilhamento de seus dados, uma funcionalidade que deverá ser liberada gradativamente, assim como a liberação dessas informações entre as instituições. Ela deverá começar pelos dados cadastrais, depois por cartões e operações de crédito.



A terceira fase dará ao cliente a possibilidade de contar com iniciação de pagamentos e receber propostas de crédito dos participantes do ecossistema. No que diz respeito aos pagamentos – que começou com o Pix – o processo se estende até setembro de 2022 quando poderá ser feito via débito em conta.

E, por fim, a quarta e última etapa, com dados públicos de serviços de credenciamento em arranjo de pagamentos, operações de câmbio, investimentos, seguro e previdência. As informações sobre as transações dos clientes nessa etapa, por sua vez, deverão começar a ser compartilhadas em maio do próximo ano.

GRANDES MUDANÇAS

Toda essa movimentação mexe com coisas importantes, desde o atual domínio de mercado dos grandes bancos até uma exposição de informações nunca antes vista, dados sendo compartilhados por empresas de portes diferentes e níveis de maturidade de segurança de dados desiguais. A preocupação atinge também o Banco Central, que estabeleceu a necessidade de adoção de protocolos de segurança, padrões e certificados de segurança.

Para especialistas desse mercado, essa atenção do BC é bem-vinda, mas é preciso ter consciência de que são medidas básicas que vão exigir um constante reforço de investimentos e políticas internas.

Para os bancos – que consolidaram há alguns anos um dos mais avançados sistemas de internet banking de todo o mundo — os investimentos em segurança são uma constante preocupação. De acordo com a pesquisa Febraban de Tecnologia Bancária 2021, tendo como base 2020, os bancos investiram R$ 2,5 bilhões em segurança cibernética, 10% do total que foi direcionado para TI.

Só para lembrar que o investimento das instituições financeiras em tecnologia – R$ 25,7 bilhões no ano passado, 8% acima do ano anterior – só fica atrás do que é aplicado pelo governo.

AS APIs NO CENTRO DAS PREOCUPAÇÕES

O setor financeiro é o principal alvo de ataques cibernéticos e o ponto crítico está ligado ao consumo de APIs

Mas ao participarem do Open Banking, essas instituições financeiras compartilharão informações com empresas que não necessariamente terão a mesma maturidade tecnológica que eles atingiram na questão da segurança de dados. E existe um ponto crítico justamente nesse compartilhamento que será feito via APIs – interfaces que permitirão interligar os diferentes sistemas dentro de um ecossistema. Para o BC, elas precisam satisfazer condições como robustez, segurança e padronização para atingirem seus objetivos nessa cadeia.

O Banco Central, inclusive, chegou a publicar um manual com normas técnicas para API onde apresenta requisitos mínimos obrigatórios para as instituições participantes e demais elementos que compõem a estrutura do Open Banking. A experiência em países mais avançados nesse processo mostra que toda atenção é necessária.

A F5 Labs, divisão da F5 Networks, realizou estudo no qual mapeou os principais incidentes de segurança de 2018 a 2020 de todas as verticais da economia e concluiu que o setor financeiro continua sendo o principal alvo de ataques e apontou ainda os riscos escondidos nos ecossistemas de Open Banking. Foram analisados sistemas de bancos abertos já operacionais na Europa, principalmente Reino Unido, além de

"O principal problema está nas engenharias sociais feitas para enganar o usuário e a ingenuidade da sociedade em relação ao mundo digital"

Flávio Gaspar
Head de produtos da Topaz

Singapura e Austrália, mais avançados com essa oferta.

A conclusão é que o ponto crítico de ataques ao Open Banking está mesmo ligado ao consumo de APIs que somente no ano passado responderam por 55% das violações. Apenas 4% de APIs em ecossistemas como varejo, governo, educação e outros são alvos de incidentes enquanto no setor financeiro esse percentual sobe para 50%.

O levantamento da F5 Labs mostra ainda que os cibercriminosos têm consciência da heterogeneidade que faz parte do Open Banking e exploram isso, principalmente com as interfaces entre *apps* móveis. O estudo relaciona que 56% da atividade criminosa focada em APIs de aplicativos móveis de finanças envolvem o roubo de credenciais, outros 11% são práticas para gerar ataques de negação de serviço DDOS.

Ainda explorando essa heterogeneidade, os cibercriminosos ao atacarem as

processadoras de pagamento têm 56% dessas tentativas como DoS. A ideia é levar um consumidor que tenta pagar um cartão de crédito a ter dificuldades com a empresa.

Por terem muito mais endereços IPs a serem atacados, as *fintechs* são alvos de todos os tipos de ataques, de tentativas de roubos de credenciais, ataques volumétricos e contra as aplicações WEB.

"As APIs vieram para dar um padrão para que os aplicativos possam conversar um com o outro. Mas é fundamental que elas sejam protegidas", comenta Maurício Ochi, gerente de contas regional da F5 Brasil. Ele completa que essa proteção é boa para o cliente, mas também para o detentor da informação que responde à Lei Geral de Proteção de Dados no caso de vazamento.

A F5 tem reforçado sua estratégia de garantir segurança nativa, já embarcada nas APIs e aplicativos. Esse foi um dos motivos que a levou a comprar a Shape Security, que ajuda a expandir essa proteção dos aplicativos e conta para isso com uma plataforma de Inteligência Artificial.

Na avaliação de Vinicius Miranda, engenheiro de soluções da empresa, há uma grande preocupação com a forma como todos estão se preparando para o Open Banking. Ele lembra que os investimentos das grandes instituições financeiras – com um forte legado – já foram e continuam sendo feitos. Mas para uma *startup* faz mais sentido entregar serviços na nuvem, com menor investimento.

"O Banco Central dá uma boa sinalização e recomendações de segurança para que as empresas possam compor o ecossistema. Mas é preciso lembrar que, além disso, outras camadas de segurança são necessárias", ressalta. Ele lembra que há vulnerabilidades das quais os participantes precisam se precaver, entre elas o limite de sucesso, ou "como me proteger do envio de códigos para dentro da minha aplicação".

Flávio Gaspar, head de produtos da Topaz – empresa do grupo Stefanini – acredita no potencial de crescimento do Open Banking no mercado brasileiro. "A Inglaterra, em dois anos, está com 10% de adesão. Aqui se estimarmos algo próximo ao que foi o Pix, essa expansão será muito mais rápida", diz. A pesquisa Febraban de Tecnologia Bancária mostrou que a expansão do Pix foi impressionante, passando de 52,9 milhões em novembro do ano passado para 338,2 milhões em março deste ano.

Na sua opinião, o Open Banking está bem regulado pelo Banco Central e Febraban (Federação Brasileira de Bancos) adotando protocolos de segurança internacionais e contando com o que há de mais moderno nessa área. Ele enfatiza que mesmo as transações via *smartphones* passam por várias camadas de segurança que ajudam a prevenir eventos.

ENGENHARIAS SOCIAIS CONTINUAM VALENDO

Mas então onde está o problema? Para Gaspar, está nas engenharias sociais feitas para enganar o usuário e a ingenuidade da sociedade em relação ao mundo digital. Hoje, como cliente de um banco, ele faz todas as suas transações no aplicativo do banco, mas, amanhã, para comprar algo na internet e fechar a aquisição no próprio *site*, sem necessidade do cartão de crédito ou do banco, é preciso ter muita confiança de que está navegando realmente no local certo.

E os *hackers*, segundo Gaspar, preferem as tramas da engenharia social que podem lhe garantir sucesso do que invadir a rede de um banco. De acordo com o executivo, isso já ficou provado na pandemia quando os cibercriminosos aproveitaram essa tática para ataque à segurança do *home office*.

De qualquer forma, a Topaz quer estar no mercado de Open Banking. A empresa lançou recentemente sistema para combate e prevenção da fraude nas transações existentes possibilitando às instituições financeiras uma visão integrada e segura para que ela possa dar uma resposta correta a transações originadas em outros canais. E vai atuar também como integradora entre sistemas aproveitando a sua especialização em *core* bancário.

COMPETIÇÃO INÉDITA

A experiência de responder pelas telecomunicações e segurança de dados da Olimpíada 2016, no Rio de Janeiro, credenciou a Embratel no mercado de combate ao cibercrime. Afinal, estima-se que naquela ocasião foram cerca de 4,2 milhões de ocorrências, dos quais mais de 730 mil ataques de negação de serviço.

A empresa já tem uma boa presença no mercado financeiro e quer estar ao lado das instituições financeiras na implantação do Open Banking e, em seguida, do Open Finance. Segundo o diretor-executivo Antonio João Filho, a Embratel conta com um amplo portfólio de segurança inclui consultoria a até mesmo assumir a área operacional de seus clientes, além de realização frequente de testes de intrusão e monitoramento dos aplicativos.

Ele considera que tanto Open Banking quanto Open Finance vão levar a uma competição inédita e interessante. Mas vai exigir cuidados redobrados. "No mundo do banco de tijolo, havia uma área de segurança patrimonial, gestão de contratos de risco. No novo mercado, essas preocupações deixaram de existir. Mas há uma outra muito mais presente: a certeza de que qualquer porta que ficar aberta será atacada pelos que passam o tempo procurando vulnerabilidades", ressalta.

"O Open Finance só pode existir porque existe a nuvem".

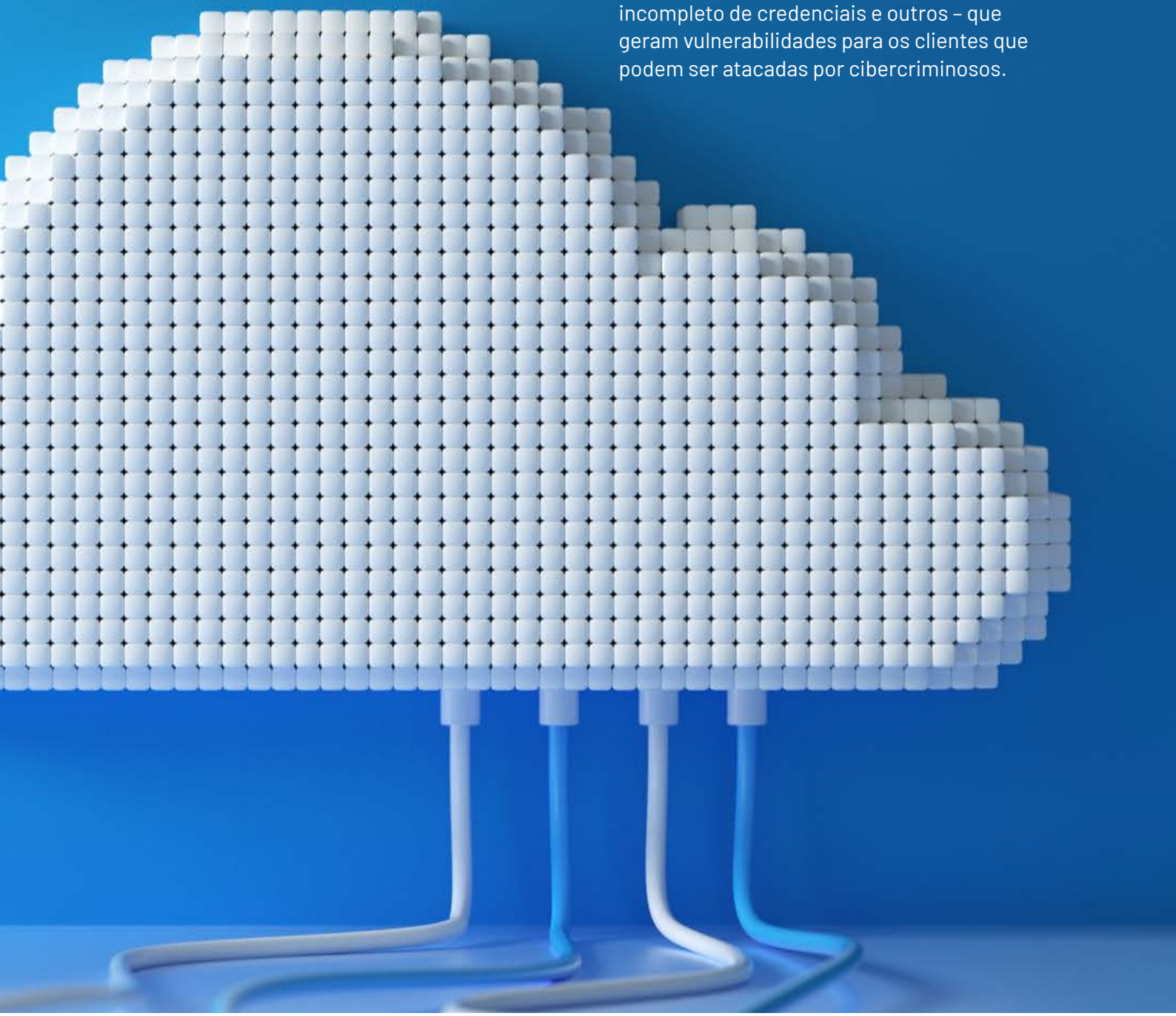
Antonio João Filho
Diretor-Executivo da Embratel

Nesse cenário, o CSO *(Chief Security Officer)* precisa antever os possíveis ataques e fazer uma avaliação diária de todos os ativos. Ele salienta que chegaremos a um cenário muito diferente do que temos hoje, com mais empresas em condições de competir com os grandes bancos. "Teremos uma grande democratização da oferta de novos serviços bancários", prevê.

Para João Filho, há um ponto fundamental em todo esse contexto: "o Open Finance só pode existir porque existe a nuvem". Inclusive os próprios sistemas de segurança rodarão futuramente em *cloud*, colocando ainda mais atenção a essa plataforma. Mas, felizmente, ele considera que houve uma evolução muito grande nessa área, o que habilita a plataforma como um dos pontos centrais dessa transição.

Um estudo divulgado pelo Gartner em julho deste ano mostra que muitos dos problemas em nuvem não são, necessariamente, responsabilidade do provedor. De acordo com o levantamento, 95% das falhas na nuvem ocorreram por culpa do próprio cliente.

Existem alguns erros comuns cometidos por eles – configurações incorretas no armazenamento dos bancos de dados, acessos remotos que ficam expostos, gerenciamento incompleto de credenciais e outros – que geram vulnerabilidades para os clientes que podem ser atacadas por cibercriminosos.



Júlio Carvalho, arquiteto de soluções especialista em segurança da Amazon Web Services, lembra que os contratos feitos com a empresa pressupõem responsabilidade compartilhada e há limites estabelecidos que não podem ser ultrapassados. Por exemplo, se o cliente leva um app para a nuvem, a responsabilidade pelos dados embarcados no aplicativo é dele.

"Na verdade, essa responsabilidade independe de onde vão ser armazenadas as informações, mas sim do tratamento dado, seja na nuvem ou em *data center*", observa.

A AWS, por sua vez, oferece um ambiente de nuvem protegido e os serviços de segurança disponíveis na plataforma. Esses serviços veêm diferentes fontes como os desenvolvidos pela própria companhia, entre os quais criptografia, controle de acesso, ou por parceiros de soluções. Mas as parcerias são mais extensas e abrangem também outras empresas que oferecem consultoria ao cliente. Essa flexibilidade tem sido um grande diferencial da companhia.

Carvalho compartilha da opinião de que o Open Finance nasceu nativo em cloud. "E estamos prontos para esse papel nesse processo de abertura do sistema financeiro", afirma o executivo. A AWS, por sinal, já chega a esse mercado com a experiência obtida em outros países nos quais o Open Banking está operacional.

No Reino Unido, por exemplo, a empresa é parceira do Starling Bank na proposta do banco inglês de se tornar uma instituição financeira que ofereça serviços com características de *marketplace*. Outra participação dos serviços da AWS está no Banco Monzo, que foi criado em 2015 totalmente em *cloud*. Com o uso da nuvem, a antiga *fintech* conseguiu ganhar escala e ajustar o custo de infraestrutura ao serviço proposto aos consumidores.

A chegada de novos parceiros financeiros nesse movimento de abertura é saudada por Carvalho como uma boa notícia para todos os que oferecem infraestrutura. "Há uma democratização saudável que permite a uma *fintech* utilizar a mesma plataforma de segurança que seu concorrente ou potencial investidor utiliza. Isso já facilita a idealização do projeto", analisa. E à AWS receber os novos atores desse mercado sem deixar de atender aos clientes já existentes.

JOGO DE XADREZ

Por mais que se diga que essa transição do mercado financeiro ocorrerá de uma forma segura, há todo um passo a passo que precisa ser conduzido com eficiência. "Como um jogo de xadrez", garante Rodrigo Fernandez, gerente de Cloud, App & Data Security da Logicalis.

Na sua avaliação, as regras do BC para Open Finance combinadas às determinações da LGPD que também terão de ser obedecidas pelos agentes financeiros exigem um movimento muito grande de governança. Nesse processo, as empresas participantes precisarão de um inventário dos ativos digitais. E não apenas inventariar, mas entender toda a

"Quanto mais novidades, mais os hackers têm ideias"

Rodrigo Fernandez
Gerente de Cloud, App & Data Security da Logicalis

aplicabilidade dessas informações. Os dados precisam ser categorizados em pessoais, sensíveis, anonimizados e semianonimizados.

O executivo acredita que do ponto de vista da governança as empresas passam a ter uma visão mais apurada da cibersegurança e como isso está relacionado aos negócios. "Nós temos na Logicalis um viés mais voltado para os negócios e primeiro buscamos saber de nossos clientes não tradicionais quais os modelos que eles adotaram para, então, determinarmos a política de segurança", diz Fernandez.

Ele reconhece que já percebe a pressão das empresas para assumirem o controle das APIs, desde sua autenticação, gerenciamento de cotas e do tráfego, entre outros itens. Para ele, os bancos estão bem preparados para dar as respostas, mas terão que conviver com as *fintechs*, que representam outro nível de maturidade tecnológica. "Quanto mais novidades, mais os *hackers* têm ideias", aposta o executivo.

OPEN INSURANCE A CAMINHO

De olho na fase do Open Banking quando se tornar Open Finance, as seguradoras começam a se preparar para entrar nesse novo modelo. A Susep (Superintendência de Seguros Privados) publicou em julho as resoluções para a implementação do Sistemas de Seguro Aberto, o Open Insurance. As normas estabelecem as condições para permitir que o consumidor acesse e compartilhe seus dados, quando desejar, com outras seguradoras e terceiros.

Com a adesão de novas empresas e serviços, os números de participantes do Open Finance no Brasil podem surpreender. Pelo menos em dois anos deverá ultrapassar a performance britânica para o mesmo prazo. Em setembro do ano passado, o sistema do Reino Unido contava com 2 milhões de cadastrados e 273 empresas conectadas.

Mas, por enquanto, no Brasil o Open Banking ainda é um quase desconhecido. Pesquisa da Febraban feita em parceria com o Ipespe (Instituto de Pesquisas Sociais, Políticas e Econômicas) revelou que 57% dos pesquisados desconhecem esse sistema. Depois de serem informados sobre o que se trata, 16% disseram que irão aderir, 30% não têm intenção de compartilhar dados financeiros e 46% ainda avaliam.

A EXPECTATIVA DO CONSUMIDOR

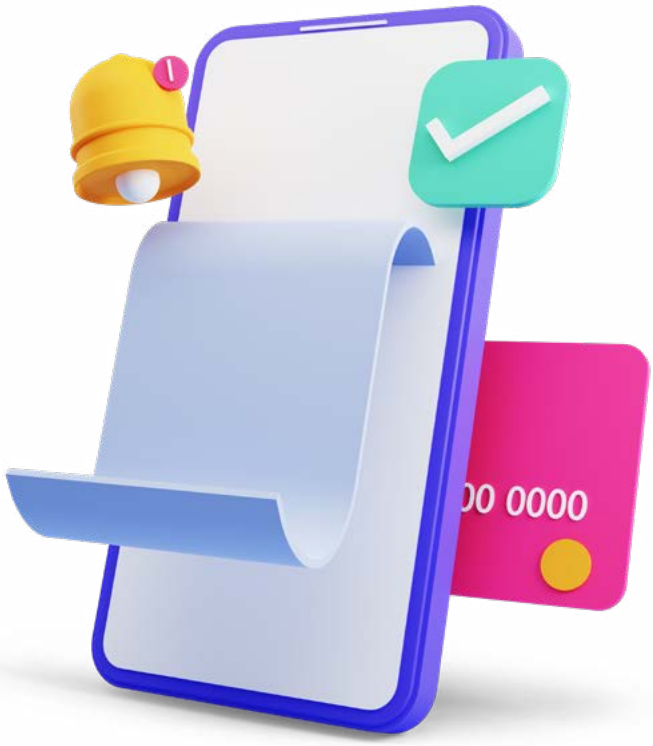
Duas pesquisas, da Mambu e Tecban, mostram como pensa o cliente bancarizado e a expectativa dos desbancarizados para o open banking

Apesar de todos os receios quando se trata de segurança da informação, o *open banking* promete aumentar a competição entre os serviços financeiros e criar oportunidades para as empresas que já estão participando do ecossistema desse mercado e para as futuras parceiras. Mas o que pensa o consumidor e quais serão suas escolhas em meio a esse cardápio de ofertas?

Duas pesquisas, uma realizada pela Tecban e outra pela Mambu, nos dão uma ideia do que se passa na cabeça dos bancarizados e dos não bancarizados sobre o comportamento do público-alvo do *open banking*. Um consenso é de que o interesse surgirá com mais intensidade de acordo com as aplicações oferecidas.

"Clientes da menor renda buscam soluções para o dia a dia"

Tiago Aguiar
Head de Novas Plataformas da Tecban



Em parceria com a Ipsos, a Tecban tem acompanhado anualmente o comportamento do consumidor no que diz respeito a serviços financeiros. A exceção foi no ano passado quando, por conta da pandemia, não foi realizado. A estratégia adotada este ano foi a de apresentar, na pesquisa, soluções de *open banking*, como agregador de contas, iniciativas de pagamento, formas de conseguir crédito mais rápido para, então, questionar a opinião dos participantes.

Cerca de 66% mostrou grande interesse pelos serviços, mas, segundo Tiago Aguiar, head de Novas Plataformas da Tecban, esse apetite também reflete uma questão de renda. Quanto maior a renda, mais atração por soluções como investimentos e, quanto menor a renda, as soluções do dia a dia, como pagamentos, atraem mais.

Uma das questões apuradas pela consulta, após a apresentação dos serviços aos consultados, referia-se à confiança das instituições. No levantamento realizado em 2018, 83% confiavam mais no banco tradicional, em 2019 esse percentual caiu para 70% e este ano foi de 73%. "O nome da instituição reverbera muito nas pessoas", observa.

Quando perguntados sobre o que esperar no futuro, 57% apontaram para proteção a fraude e poder se conectar a uma pessoa caso algum problema ocorra, resposta superior ao 52% de 2019. Aguiar chama a atenção para outra aplicação que também registrou importante crescimento: pagar contas pelo app passou de 43% em 2019 para 50%.

ACESSIBILIDADE FINANCEIRA

Já a pesquisa realizada pela Mambu – empresa com plataforma SaaS em nuvem – mostra que ainda há muito para avançar. Para começar,

"Os bancarizados também não se sentem bem atendidos"

Sergio Constantini
Diretor-geral da Mambu

42,5% dos que responderam ao levantamento confessaram que vão buscar conselho na internet sobre investimentos, enquanto apenas 19,2% recorrem ao executivo do banco.

Para o diretor-geral da empresa, Sergio Constantini, o maior mérito do Open Finance é justamente o de abrir oportunidades a partir do momento que se coloca o cliente no centro dos negócios.

A acessibilidade financeira, tema da pesquisa da companhia, dá muitas pistas do universo que o ecossistema de Open Finance poderá explorar. Para aqueles que apostam que a principal causa do elevado número de

desbancarizados está na falta de capital, chegou próximo. O levantamento mostra que 17,1% dos participantes alegam ser esse o motivo. Mas há um percentual maior, 29,9%, que não apresenta nenhuma causa para isso, posicionando-se sem motivos particulares para não ter a conta bancária.

A falta de acesso à tecnologia é relatada por 3,4% dos desbancarizados que participaram do levantamento, 8,5% dizem que não sabem como abrir uma conta, 6,8% reclamam que estão longe das agências e 8,5% comentam que não precisam de uma conta bancária.

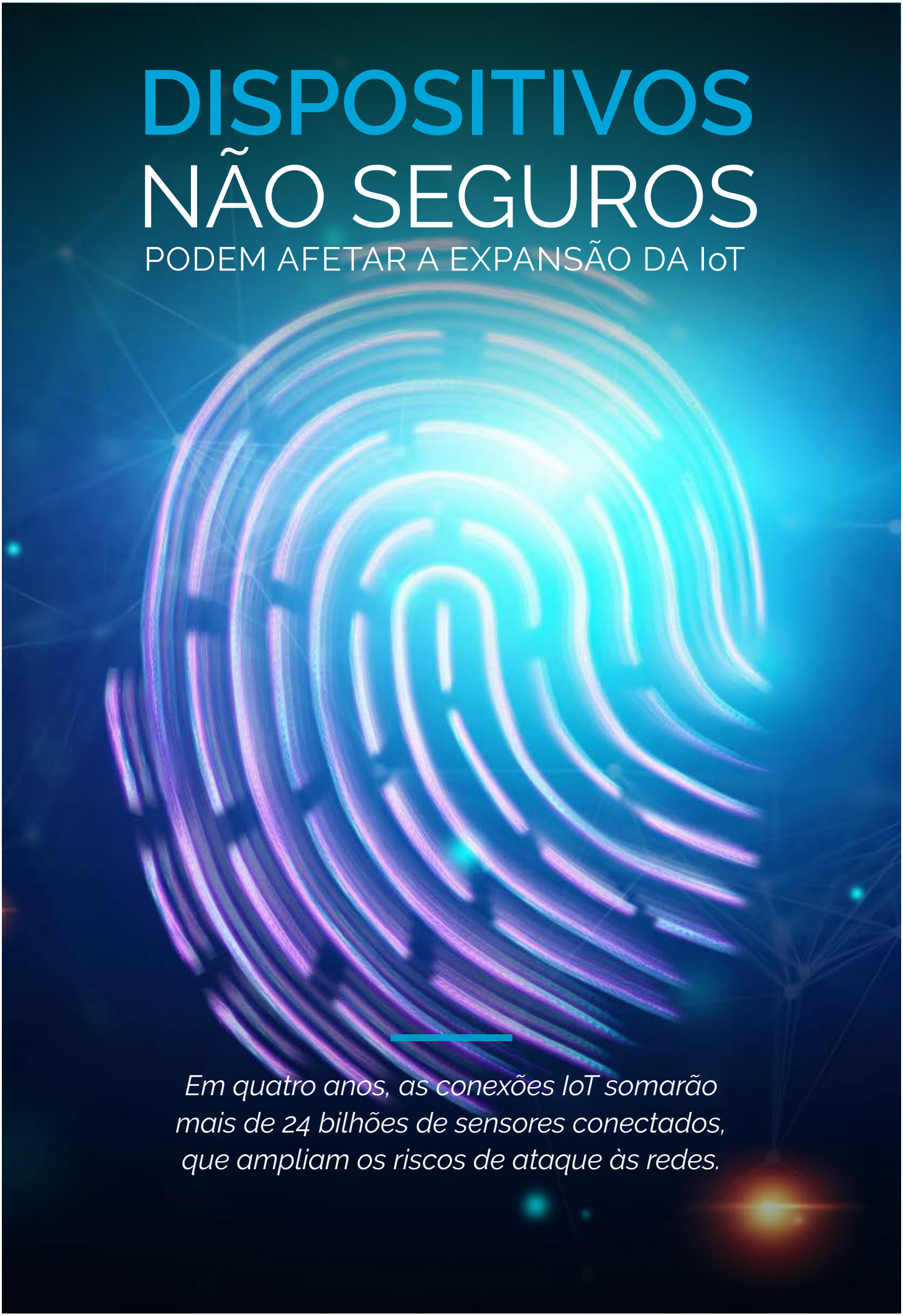
O fato de recorrerem pouco ao gerente do banco tem reflexo em outra questão da pesquisa da Mambu. 60% admitiram que teriam uma situação financeira melhor se tivessem mais informações sobre como o sistema financeiro funciona. "O que mais me impressionou no resultado foi o de que os bancarizados não se sentem bem atendidos", chamou a atenção Constantini.

Na sua avaliação, é preciso que as instituições passem de generalistas para mais especialistas, atendendo adequadamente os diversos nichos do mercado de correntistas e pessoas que poderão se ligar ao mercado financeiro, criando soluções específicas para todos os perfis de clientes. Ele lembra que não é possível sustentar a acessibilidade financeira sem baixo custo e isso precisa estar no meio das estratégias de Open Finance. "Até agora nós temos nesse processo apenas a ponta do *iceberg* das oportunidades financeiras", declarou o executivo.

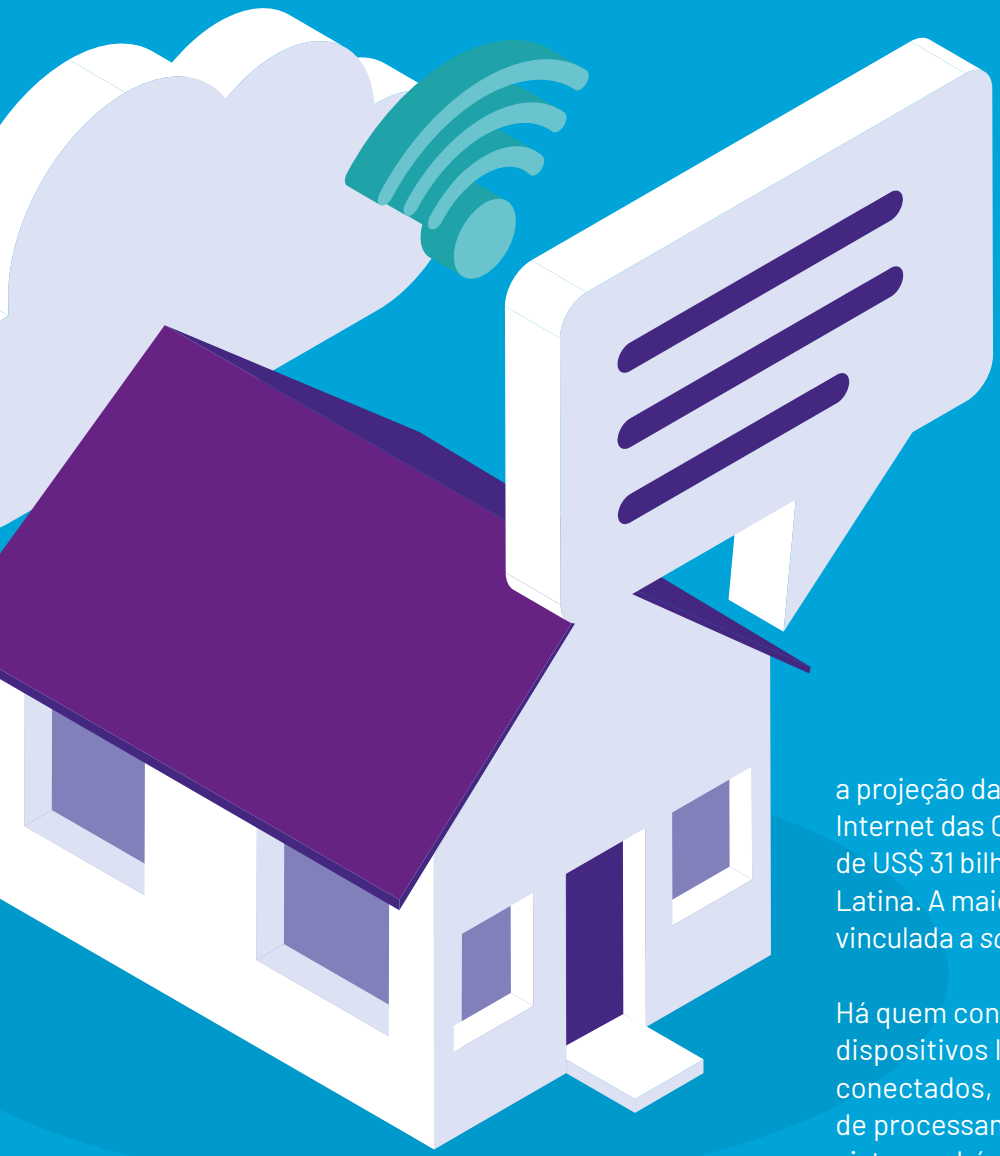

HUAWEI
23 ANOS
NO BRASIL PARA O BRASIL
HUAWEI E BRASIL
23 ANOS
DE CONEXÃO E PARCERIA
PARCEIROS NO PRESENTE, PARCEIROS NO FUTURO.

DISPOSITIVOS NÃO SEGUROS

PODEM AFETAR A EXPANSÃO DA IoT



Em quatro anos, as conexões IoT somarão mais de 24 bilhões de sensores conectados, que ampliam os riscos de ataque às redes.



Quando falamos de Internet das Coisas (IoT) quase sempre vem à nossa mente milhões de dispositivos distribuídos em praticamente todos os setores econômicos. Eles estão, ou estarão, nas casas conectadas, nos carros autônomos, nos aviões, nos meios de pagamento, nas cidades inteligentes, na Indústria 4.0, na agricultura, nos portos, aeroportos e estradas, nos governos, nos hospitais e em uma série de outras aplicações, inclusive em áreas de infraestruturas críticas, como energia, óleo e gás. Já para aqueles que trabalham com segurança de dados e formas de combater ciberataques, vulnerabilidades em ritmo acelerado são imediatamente associadas a esses dispositivos.

Os números referentes à IoT são sempre grandiosos. Em quatro anos, o total de conexões poderá passar dos atuais 13,3 bilhões de acessos para algo como 24 bilhões, como aposta a entidade GSMA. Em termos de valores, a projeção da GlobalData é de que o mercado de Internet das Coisas poderá movimentar cerca de US$ 31 bilhões até 2023 somente na América Latina. A maior parte desses recursos estará vinculada a *software* e serviços.

Há quem considere que, por natureza, os dispositivos IoT são inseguros. Eles estão conectados, mas não possuem capacidade de processamento suficiente para carregar sistemas básicos de proteção, como a criptografia. O que significa, em tese, que podem causar estragos consideráveis.

Os alertas do que um ataque IoT pode causar não faltam. Desde os mais antigos, como o vazamento de dados de 40 milhões de cartões de crédito de clientes da rede de supermercados Target, que foi iniciado por um acesso remoto do ar-condicionado conectado na rede, até os mais recentes, como a temerária invasão de um centro de tratamento na Flórida para alterar perigosamente a composição da água que abasteceria uma cidade.

No entanto, muitas vezes pelo grande número de dispositivos utilizados – há sensores baratos que são instalados na rede até sem o conhecimento da TI – ou por que o produto não valoriza as vulnerabilidades corretamente, a segurança de IoT foi por muito tempo negligenciada. E os cibercriminosos sabem disso e veem nesse mercado um terreno fértil.

DA FÁBRICA, SEM SENHA

"A atualização de cada dispositivo deve ser contínua por todo o tempo de vida", alerta Sergio Ribeiro, consultor Sênior de Segurança da Informação do CPQD

"Esses dispositivos aumentam a superfície de ataque", observa Sergio Ribeiro, consultor Sênior de Segurança da Informação do CPQD. Ele ressalta que muitos desses equipamentos vêm de fábrica com uma senha fraca ou mesmo sem nenhuma. Como um dos procedimentos básicos, essa senha teria de ser reforçada assim que passa a se conectar na rede, mas nem sempre isso é feito, causando vulnerabilidades.

As formas de tornar esses dispositivos seguros são muitas vezes negligenciadas pelos próprios fabricantes ou pelas empresas que os adquirem. "Se ele está na rede, tem de ser cuidado com atenção", acrescenta.

Ribeiro elenca outro problema, referente às atualizações desses equipamentos, que são feitas apenas dentro de uma janela de tempo determinada e abandonadas em seguida. "Se o dispositivo tem *software* embutido, deveria ter atualização contínua por seu tempo de vida. Mesmo em casa, uma *smart* TV que deixa de ter atualização torna-se uma vulnerabilidade e isso é o que também acontece nas empresas", ressalta.

O primeiro passo para garantir a segurança é realizar um inventário de todos os elementos que estão conectados na rede. Isso inclui um apurado levantamento sobre as versões que estão rodando, se o produto foi descontinuado, quais as atualizações disponíveis, entre outros.

"Esse inventário precisa ser bem realista para preservar os demais dados"

Sergio Ribeiro
Consultor Sênior de Segurança da Informação do CPQD

"Esse inventário precisa ser bem realista para preservar os demais dados", observou. Ribeiro também orienta para que se apliquem camadas de proteção, com uma rede segregada, protegida.

A gravidade desses ataques aumenta à medida que infraestruturas críticas incrementam o uso de mais sensores de automação. Desde março do ano passado, por exemplo, estiveram sob ataque cinco empresas de energia: Enel, EDP, Light, Copel e Eletronuclear. As ações não tiveram consequências sobre distribuição e fornecimento de energia, mas afetaram sistemas administrativos e houve vazamento de informações.

EM TODOS OS LUGARES

Muitas vezes o perigo está onde menos se espera. A Blockbit, empresa que faz testes de segurança nos aparelhos digitais de seus clientes, também simula riscos e potencial de fraudes para demonstrar como os riscos estão muito presentes. Por exemplo, recentemente em uma empresa de pecuária, a Blockbit conseguiu invadir a balança industrial inteligente do cliente e alterar o peso dos bois, o que poderia gerar um grande prejuízo ao produtor caso esse ataque fosse mesmo intencional.

"A segurança por design, que implementa requisitos de segurança desde a primeira etapa do projeto, é uma das formas de proteção desse ambiente"

Wolmer Godoi
Diretor de Tecnologia da Blockbit

Wolmer Godoi, diretor de Tecnologia da Blockbit, avalia que são poucas as empresas que se preocupam com todo o sistema que utilizam. E precisam ainda lidar com dispositivos pulverizados e com a dificuldade de formação de especialistas. Ele admite que há dificuldade de realizar um inventário adequado no qual todos os dispositivos, de uma catraca eletrônica inteligente a câmeras de segurança, precisam estar relacionados. Mas, sem dúvida, é preciso fazê-lo, alerta.

Lembra que à medida em que aumenta o uso desses equipamentos em áreas críticas, esses dispositivos podem perigosamente comprometer vidas, e em breve serão encontrados em carros autônomos, em hospitais ou usinas.

Godoi observa que manter uma rede de IoT desconectada da internet – como as urnas eletrônicas utilizadas nas eleições brasileiras – é uma forma de proteção desse ambiente. Assinala que começam a ser cogitadas outras soluções, como segurança por *design*. Essa solução tem como conceito o de se levar em conta a segurança da informação durante o processo de desenvolvimento de um produto. Ou seja, desenvolver um *hardware* ou *software* para torná-los o mais livre possível de vulnerabilidades, adotando requisitos de segurança desde as primeiras etapas do projeto

Para o usuário doméstico também há riscos. Um estudo realizado pela Avast e Universidade de Stanford em 16 milhões de lares em todo o mundo mostrou que muitos aparelhos funcionam com as senhas que vieram de fábrica. Além disso, ainda há em grande escala o uso de protocolos antigos com muitas vulnerabilidades.

Os exemplos são inúmeros. Pesquisadores do Laboratório de IoT da Avast, por exemplo, encontraram falhas de segurança em *set-top* boxes usados pelo consumidor final. De marcas como Philips e Thomson, esses equipamentos conectados à internet operam com portas abertas, utilizando protocolo não criptografado com mais de 50 anos de uso.

Com o foco nesse mercado, a Blockbit desenvolveu soluções específicas para proteção de plataformas IoT que estão sendo exportadas. A empresa tem produtos na França, Espanha, Reino Unido, Chile e Colômbia.

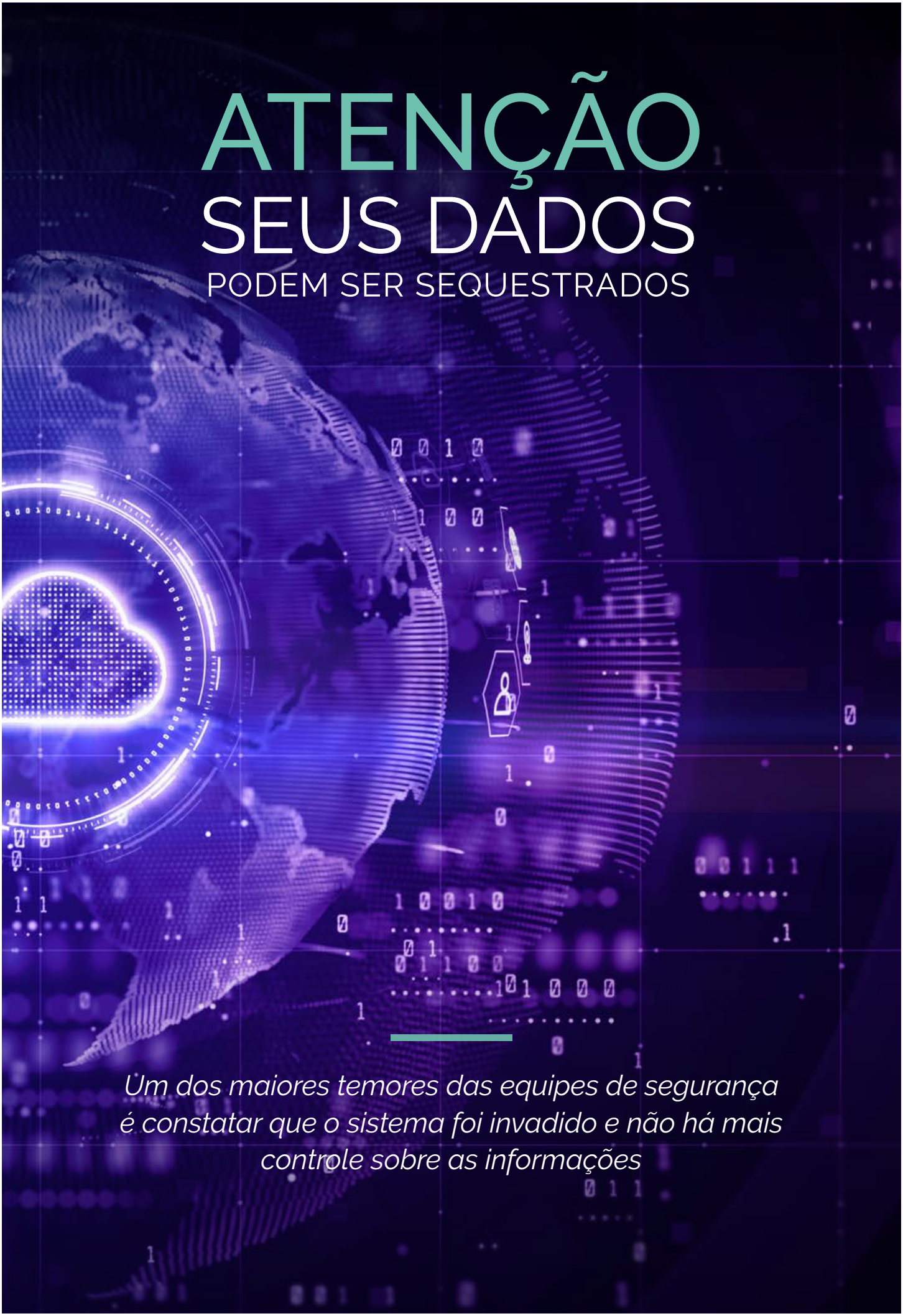
WANNACRY E MIRAI, OS FANTASMAS

Na avaliação de Godoi as empresas começaram a se preocupar mais com a segurança completa em todos os ativos a partir de eventos de cibercrime que tiveram repercussão mundial. Um deles foi conhecido como WannaCry, uma família de *malwares* que afetou mais de 200 mil computadores de todo o mundo utilizando uma falha no sistema operacional que foi vazada pela NSA, Agência de Segurança Nacional dos Estados Unidos.

No mundo específico de IoT o primeiro grande susto ocorreu há cerca de 5 anos com o *botlet* Mirai. Ele foi responsável pelo maior ataque DdoS, gerando um tráfego de 1,2 Tbps contra o provedor DNS, Dyn. O *malware* transformou dispositivos IoT que rodavam Linux em um exército de *bots*, principalmente câmeras de segurança e roteadores. Era como um "exército de zumbis", como foi chamado na ocasião, sendo operados remotamente para negação de serviço do alvo escolhido pelos *hackers*.

Os exemplos se multiplicam nesse mercado à medida em que o número de equipamentos cresce. No ano passado, a IBM divulgou a descoberta de uma falha de segurança em uma série de *chips* de conectividade IoT que poderia deixar bilhões de dispositivos vulneráveis à invasão.

Com toda essa preocupação, e movimentação, o mercado de segurança de IoT tem se mostrado aquecido. Relatório da Million Insights aponta para uma receita global de US$ 9,88 bilhões até 2025. De acordo com o Gartner, os gastos com segurança de IoT nos terminais este ano alcançará algo como US$ 631 milhões.


ATENÇÃO
SEUS DADOS
PODEM SER SEQUESTRADOS
Um dos maiores temores das equipes de segurança é constatar que o sistema foi invadido e não há mais controle sobre as informações

Existem várias formas de ataque a uma rede de computadores por cibercriminosos. Mas o aviso de que seus dados foram sequestrados, criptografados – portanto você não terá mais acesso — e só serão liberados mediante um pagamento – muitas vezes em criptomoeda – é, sem dúvida, um dos mais aterrorizantes. É o *ransomware* entrando na vida de sua empresa.

Podem transcorrer dias ou mesmo semanas que, dependendo do que foi atingido, até as atividades mais simples vão estar vinculadas a esse evento. É possível evitá-lo? Sim, é. Mas é preciso ter a cultura de segurança impregnada em toda a estrutura corporativa.

Considerado um dos tipos mais prejudiciais de *malwares*, o *ransomware* pode agir bloqueando a tela para o usuário ou encriptando os arquivos. De qualquer forma, o cibercriminoso assume o comando das máquinas e pode tanto destruir dados quanto cobrar para o resgate das informações sequestradas.

Para aqueles que possuem um *backup* completo de tudo que está no sistema é mais fácil agir desligando as máquinas e as religando sob o que está copiado. Mas quantas empresas podem garantir que possuem esse recurso atualizado? Ou possuem sistemas capazes de detectar a silenciosa invasão a tempo de tomar as providências?

Nos últimos anos, os ataques de *ransomware* crescem a taxas assustadoras. Uma pesquisa da IDC publicada em agosto mostra que mais de um terço das organizações em todo o mundo sofreram um ataque ou violação desse *malware*.

Os setores com maior incidência foram os de finanças e manufatura. E apenas 13% disseram que sofreram um ataque ou violação e não pagaram resgate. A média mundial desses pagamentos é da ordem de um quarto de milhão de dólares, mas alguns pagamentos chegaram a superar US$ 1 milhão.

MAIOR INCIDÊNCIA NA PANDEMIA

Alguns ataques tornaram-se mais conhecidos. Entre eles, o que atingiu a multinacional brasileira JBS e o que afetou o grupo Colonial Pipe, nos Estados Unidos

A pandemia tornou-se um terreno fértil para vários ataques de segurança, incluindo *ransonware*. Levantamento feito pela SonicWall aponta que no primeiro semestre deste ano os ataques superaram as incidências de todo o ano passado. Somente em junho foram 78,4 milhões de incidentes.

Cinco países foram atacados de forma massiva: Estados Unidos, Reino Unido, Alemanha, África do Sul e Brasil. De acordo com o levantamento, três famílias de *ransomware* – Riuk, Cerber e Samsam – responderam por 64% de todos os ataques.

Em geral, as empresas procuram restringir as informações sobre os ataques recebidos a grupos específicos de segurança a fim de não afetarem a imagem das marcas. Mas, se ocorrer o vazamento de dados de terceiros, são obrigadas a divulgar as informações para as autoridades e para o público.

Durante a pandemia, alguns casos ficaram famosos. Nos Estados Unidos, o ataque à multinacional de origem brasileira JBS está, sem dúvida, entre eles. Os ataques seriam de responsabilidade do grupo de cibercriminosos mais atuante do mundo, o Revil, que segundo o FBI, esse grupo utiliza táticas sofisticadas e especializadas.

A JBS descobriu o ataque em maio deste ano em suas unidades norte-americanas e australiana e foi forçada a fechar todas as unidades processadoras de carne nos Estados Unidos. A empresa alega que conseguiu resolver o problema na maior parte de seus bancos de dados. Mas, ao que tudo indica, dois deles não puderam ser salvos, o que teria obrigado a empresa a pagar US$ 11 milhões para não comprometer as demais informações. O pagamento teria sido feito em *bitcoin*.

Apesar da orientação do governo estadunidense para que não se efetuem pagamentos aos cibercriminosos, outro caso famoso também ocorrido em maio no país foi registrado. O grupo Colonial Pipeline, que transporta 45% do combustível na Costa Leste dos Estados Unidos teve de interromper o fornecimento devido ao ataque de *ransomware*.

Os *hackers* pediram cerca de US$ 4,4 milhões, que também teriam sido pagos, para que a empresa pudesse reiniciar sua rede de oleodutos. Comenta-se que o pagamento, também feito em *bitcoins*, foi parcialmente recuperado pelo FBI.

SAÚDE TAMBÉM É ALVO

Mas não é preciso mirar para fora do país para saber quão nocivos os ataques *ransomware* podem ser. O grupo Fleury, maior grupo de diagnóstico do Brasil e com mais de 200 centros de atendimento no mundo, foi alvo de *hackers* em junho deste ano. Os clientes que fizeram exames em suas clínicas tiveram grandes dificuldades de resgatar os resultados *online* e mesmo o *app* que foi criado pela empresa durante o período emergencial passou por instabilidades.

O laboratório levou cerca de uma semana para restabelecer o acesso aos exames, assim como para fazer funcionar a central de atendimento em sua integralidade. Na *deep web* – uma zona da internet que não pode ser facilmente detectada por mecanismos de busca – circularam rumores de que o Revil teria reivindicado a ação.

"Ninguém está 100% protegido, por isso é fundamental ter uma gestão baseada em risco"

Arthur Capella
Country manager da Tenable Brasil

O laboratório não confirmou se foi vítima de *ransonware*, apenas concordou que foi vítima de ataques. Mas garantiu que a base de dados permaneceu íntegra e que informações não foram vazadas. Para apurar o acontecido, montou uma força-tarefa reunindo cinco empresas, IBM, Microsoft, Accenture, PWC e Proteus.

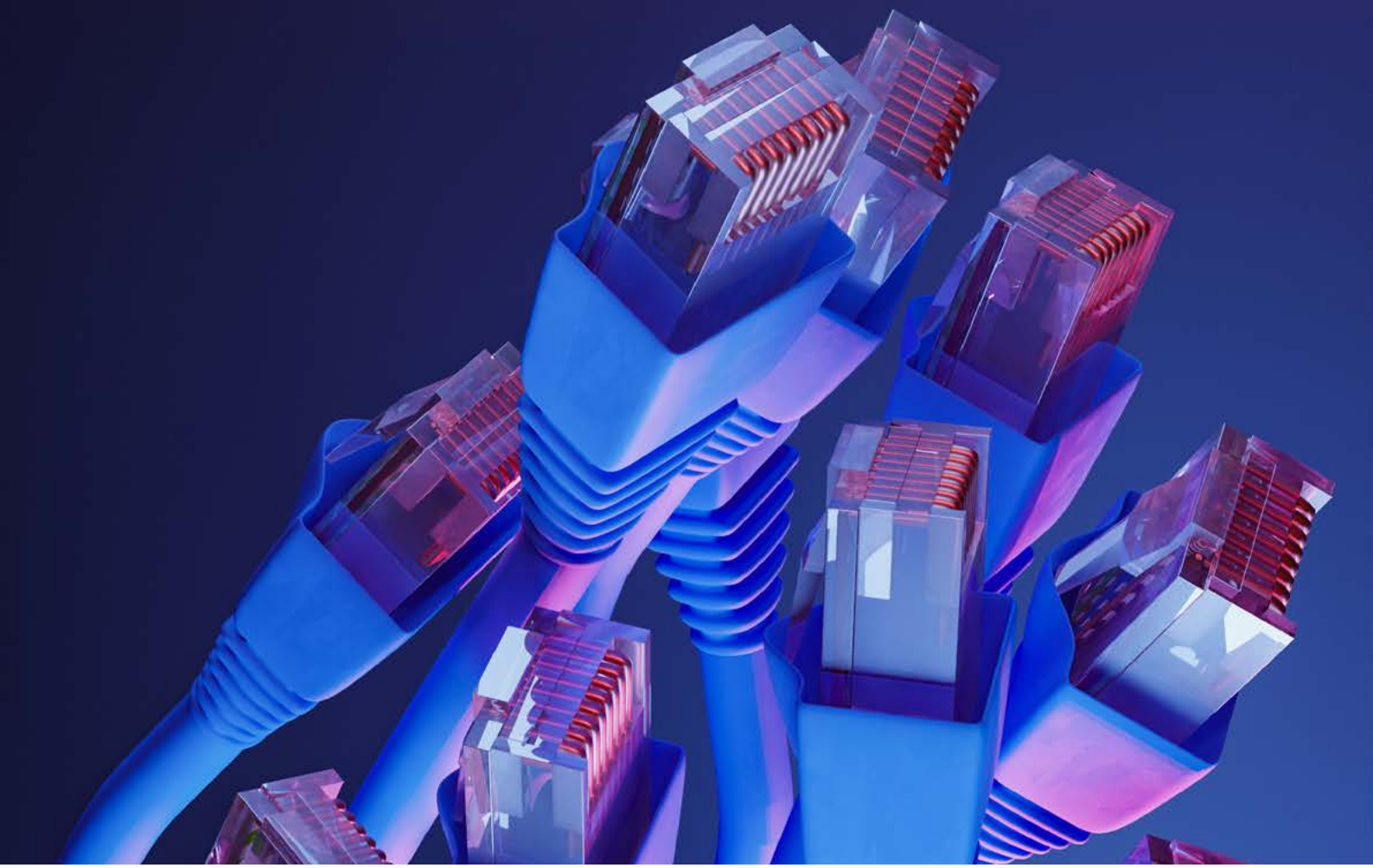
"Ninguém está 100% protegido, por isso é fundamental ter uma gestão baseada em risco para proteger o que gera mais impacto para o negócio", observa Arthur Capella, country manager da Tenable Brasil. Na sua avaliação, os ataques à JBS e à Colonial Pipeline inauguram uma nova era do crime digital não apenas porque foram extremamente rentáveis, mas também por afetarem consumidores em grande escala.

Cada empresa deve definir as prioridades que precisam ser protegidas e, para isso, criar um mapa com a visibilidade de todas as atividades operacionais e de tecnologia.

A integração da TI com as áreas operacionais e de negócios também é uma das necessidades prementes nesse processo, na avaliação do executivo.

Capella lembra que, a cada inovação que chega ao mercado, muitas vulnerabilidades surgem, até que a tecnologia seja dominada e permita novas normas de segurança. Foi assim, por exemplo, com os dispositivos móveis, com a *cloud* e virá com as demais tecnologias, como IoT (Internet das Coisas) e 5G.

Ele observa que muitos ambientes industriais possuem um *mix* de dispositivos que nem sempre são de conhecimento da área de TI, o que torna difícil um programa de gerenciamento de *patches* atualizado. Em áreas críticas, é necessário um sincronismo entre o gerenciamento de *patches* e as vulnerabilidades que estão sendo descobertas.



"Os desenvolvedores não costumam utilizar sistemas seguros para o desenho das *apps*"

Alexandre Murakami
Diretor Latam da Unidade de Segurança da Logicalis

MONITORAMENTO CONTÍNUO

Alexandre Murakami, diretor Latam da Unidade de Segurança da Logicalis, mantém o otimismo. Ele lembra o ano de 2000, quando a segurança cibernética não estava entre as maiores preocupações dos executivos. "Poucos profissionais de segurança de informação eram contratados e hoje evoluímos significativamente com muitos talentos nessa área", observa.

Ele reconhece, entretanto, que o número de incidentes tem crescido bastante na última década, principalmente nos últimos cinco anos. Mas ainda é difícil dimensionar o tamanho do prejuízo que causam, uma vez que o sigilo continua imperando entre os atingidos. "É possível tratar do assunto com os fornecedores de segurança envolvidos. Mas pouco se abre, por exemplo, sobre o pagamento pelo sequestro dos dados", diz.

Ele sugere algumas medidas que podem ser tomadas pelas empresas que ajudam a evitar invasões. Entre elas, procurar utilizar dupla autenticação e não operar com senhas fracas, como tem sido padrão em muitas companhias.

Murakami chama a atenção para o fato de que há muitas vulnerabilidades na camada de aplicação. "Os desenvolvedores não costumam utilizar sistemas seguros para o desenho dos *apps*, deixando brechas facilmente encontradas pelos cibercriminosos", afirma.

O executivo também concorda com a necessidade de boa gestão dos *patches*. Nesse conjunto de medidas, aponta que também é necessário implementar *EDRs (Endpoint Detection and Response*), tecnologia que monitora e responde continuamente para mitigar ameaças cibernéticas.

"O monitoramento constante da infraestrutura é importante, é preciso descobrir o mais rápido possível quando há uma invasão, para que possam ser tomadas providências de resposta ao ataque, preservação dos bancos de dados e outras providências", enfatiza. Nesse processo, são bons aliados a inteligência artificial e *machine learning*, inclusive para detectar se alguma parte do sistema está consumindo recursos de forma diferente e se há correlação entre esses incidentes.

QUANDO O MUNDO CORPORATIVO ESTREMECEU

A pandemia que obrigou milhares de trabalhadores a serem realocados para home office e expôs a necessidade de aumentar investimentos em segurança

O ciberataque às lojas Renner, somado a outros incidentes recentes, abalou as estruturas do mundo corporativo. Não porque tenha sido o primeiro nesse período pandêmico, mas pela disposição dos atacantes de estenderem a atuação para novas áreas, como as grandes redes de comércio. Tudo isso em um tempo que a própria pandemia trouxe a necessidade de garantir a segurança do *home office* e quando as multas previstas na LGPD (Lei Geral de Proteção de Dados) por vazamento de informações começaram a ser aplicadas. Ou seja, o caldeirão começou a ferver.

O caso das lojas Renner foi identificado como mais um ataque de ransomware, um dos mais perigosos, e uma vez que o sistema da empresa é invadido as informações são criptografadas pelo atacante e é pedido um resgate pela liberação dos dados.

Em comunicado, a Renner garantiu que não teve nenhum contato com os atacantes e não pagou resgate. Também afirmou que os principais bancos de dados foram preservados. Os canais *online* da companhia ficaram fora do ar por no mínimo 48 horas e o *site* do Camicado, do mesmo grupo, também foi afetado.

O incidente da Renner se soma a outros de grande porte, como os ataques ao grupo de diagnóstico Fleury e à Embraer, que chegou a ter documentos vazados que estavam em "determinados ambientes", como disse a empresa. Ela desativou partes dos servidores e teve de operar sob norma de contingência. Ambos também negam terem pago para resgatar as informações.

Uma pesquisa da Check Point Research, braço de Inteligência em Ameaças da Check Point, concluiu que no ano passado o ransomware custou às empresas em todo o mundo cerca de US$ 20 bilhões, 75% a mais que 2019. Globalmente os setores mais atacados foram saúde, *utilities*, seguros e judiciário.

Em abril deste ano, a pesquisa da Check Point mostrou que o Brasil superou a média mensal global de ataques de ransomware, com 3,1% contra 2%. Nesse período, a vulnerabilidade mais comumente explorada no país foi o Remote Code Execution, pelo qual o *hacker* executa remotamente um código malicioso.

Com a pandemia e a necessidade de realocar funcionários rapidamente para o *home office*, o acesso remoto entrou no olho do furacão. Outra pesquisa, dessa vez da Kaspersky, diz que em fevereiro de 2020 o Brasil registrava 11,6 milhões de incidentes contra o protocolo de área remota de trabalho e no mês seguinte, quando a pandemia teve início, já eram 35,5 milhões, um crescimento de 204%, acima da média global que foi de 197%.

De acordo com o alerta da Kaspersky, depois disso os incidentes nunca ficaram abaixo de 20 milhões e em janeiro e fevereiro deste ano foram registrados mais de 56 milhões de ataques.

INTERNET CRESCEU EM TRÁFEGO E PERFIL DE USO

"Com a pandemia algumas atividades na internet cresceram acima dos padrões normais de uso. E chegamos a registrar aumento de tráfego de 30% em dois meses que, normalmente, é a média de um ano", observa Claudio Baumann, diretor-geral da Akamai no Brasil. Ele cita como exemplo os games, cujo uso expandiu 160% no início da pandemia, as redes sociais tiveram mais de 60% de acessos. "E as tentativas maliciosas aumentaram mais de 400%", observa.

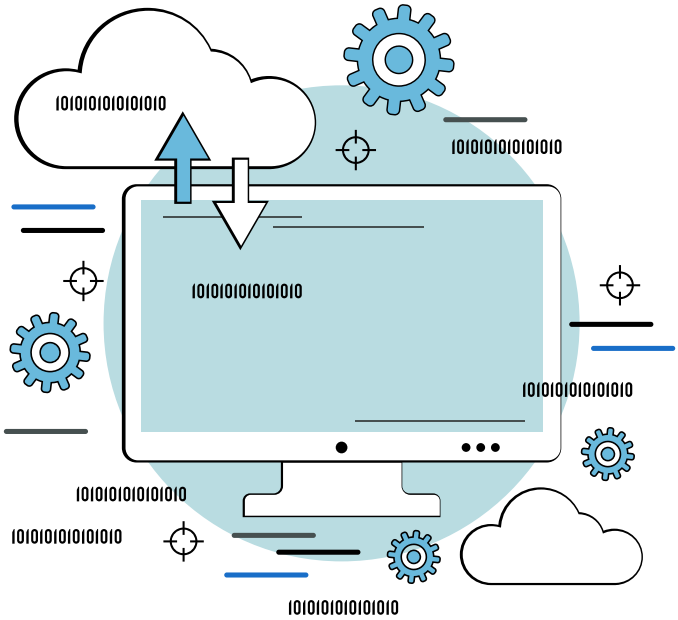
Ele relata que, independentemente do tipo de ameaça, houve crescimento de ataques. Os incidentes DDOS, por exemplo, aumentaram 34%. " Só que houve uma diferença. Esses incidentes ocorreram com mais sofisticação e volumes maiores. Somente no primeiro trimestre mitigamos quase 2 mil ataques DDOS", afirma.

O executivo conta que as empresas, em primeiro lugar, adotaram redes VPNs para cobertura de parte dos empregados em suas residências, estabelecendo parâmetros para o acesso remoto. Mas, ele lembra que essa solução não atendeu todos os funcionários, deixando algumas brechas.

"As tentativas maliciosas aumentaram mais de 400%"

Claudio Baumann
Diretor-geral da Akamai no Brasil

As empresas perceberam, então, que eram necessárias camadas adicionais e ferramentas de segurança. "Muitos me perguntam o que devem fazer, mas a resposta não é linear, não é única para todos. Existem ferramentas potentes, claro, mas é preciso também fazer análise dos seus pontos vulneráveis e definir qual a melhor política de segurança para seu perfil de negócios, entender os riscos, o que possuem de mais precioso", analisa.



O FIM DO PERÍMETRO

Luiz Karl, data protection officer (DPO) da ClearSale, chama a atenção para o benefício das análises comportamentais

"Isso é algo que vem mexendo nos negócios e na forma de ver a segurança de dados. Há multas para aqueles que deixarem acontecer esse tipo de ocorrência"

Luiz Karl
Data protection officer (DPO) da ClearSale

Para Luiz Karl, officer (DPO) da ClearSale, o primeiro impacto do *home office* foi justamente terminar com o perímetro de segurança com o qual as empresas trabalhavam. Se antes, trabalhar fora da empresa era uma prática esporádica, com a pandemia tudo foi alterado e preocupou ainda mais as equipes de segurança.

Outros eventos se somaram a esse. O uso de nuvem já era uma tendência crescente e colaborava para mudar o centro de dados que antes estava perto fisicamente. E as multas da LGPD já estavam a caminho e foram consolidadas em agosto deste ano.

Enfim, havia muito por fazer. Karl chama a atenção para o benefício das análises comportamentais que, nesse caso, não seriam unicamente de pessoas mas de equipamentos. Para isso, há um *mix* tecnológico que ajuda a captar qualquer mudança de comportamento e bloquear o dispositivo em questão, como biometria, geolocalização e outros recursos.

Nos projetos de segurança, as validações estão sempre subindo um degrau para que seja possível avaliar os riscos residuais. Na sua avaliação, as medidas de controle já vinham sendo implantadas pelas empresas, mas a pandemia acelerou processos.

O executivo lembra que o *e-commerce*, muito mais utilizado no período pandêmico em todo o país, acelerou projetos contra a fraude e ficou mais protegido. Foram desenvolvidos sistemas para identificar o tipo de compra que está sendo feita, de acordo com o padrão usual do cliente e, se houve alguma alteração, perceber qual o alvo e acionar os mecanismos de segurança.

O MEDO DOS VAZAMENTOS (E DAS MULTAS)

Na sua opinião, as empresas também se preocuparam muito em garantir todos os requisitos para evitar vazamentos e atender à LGPD. "Isso é algo que vem mexendo nos negócios e na forma de ver a segurança de dados. Há multas para aqueles que deixarem acontecer esse tipo de ocorrência."

As corporações, inclusive, criaram cargos como o encarregado dos dados, ou mesmo equipes voltadas para isso. E, de quebra, o mercado de empresas e consultorias voltadas para segurança se mantém aquecido.

Fabio Soto, CEO da Agility, não tem dúvidas de que a migração para nuvem atingirá empresas de todos os portes em um caminho sem volta. A própria empresa possui grandes, mas também médias companhias em sua carteira de clientes que se preocupam com uma solução de proteção *multicloud* que lhes dê visibilidade de tudo que é relacionado a esse tema, como vulnerabilidades no código ou estrutura nas nuvens, integração de plataformas, entre outros.

"Segurança é um processo no qual vamos colocando camadas, estruturando políticas, endereçando determinados tipos de ameaças, acompanhando em tempo real todos esses sistemas"

Paulo Venâncio
Diretor de Pré-Vendas de Soluções Digitais da Embratel

"Todos estão precisando cada vez mais desse apoio", ressaltou o executivo. Ele também chama a atenção para a necessidade de proteção das aplicações, cada vez mais onipresentes no mundo dos negócios. Ressalta que a segurança tem de estar no *app* desde o início, ainda na codificação, dentro de um processo automatizado com parâmetros de proteção. E é preciso continuar se preocupando com todo o ciclo de vida desse *app* como faz parte da infraestrutura da nuvem.

"Segurança é um processo no qual vamos colocando camadas, estruturando políticas, endereçando determinados tipos de ameaças, acompanhando em tempo real todos esses sistemas", observa Paulo Venâncio, diretor de Pré-Vendas de Soluções Digitais da Embratel.

LGPD COLABORA PARA A PREVENÇÃO

"Focamos em quase uma dezena de verticais", afirma Marcelo Motta, diretor de Cibersegurança e Soluções da Huawei para a América Latina.

Ele explica que, no trabalho de consultoria que a empresa presta, observa que muitas empresas acreditam que estão protegidas, mas, na verdade, não possuem a maturidade de segurança de dados. "Elas têm mais sorte do que uma proteção efetiva. Com a ausência de eventos, creem que estão seguras", comenta.

A maturidade pressupõe um olhar crítico sobre todo o sistema, de forma contínua, com análise de vulnerabilidade e gestão recorrente sobre o comportamento da rede, dos usuários.
A Embratel tem apostado, inclusive, em novas tecnologias como Inteligência Artificial para ajudar nesse processo.

Na visão de Venâncio, a LGPD colaborou de alguma forma para fortalecer o tema da prevenção dentro das empresas, principalmente médias e pequenas que ainda não tinham se debruçado sobre essa questão. Ainda como efeito da lei no mundo corporativo, o executivo ressalta que a prevenção de vazamento dos dados não ficou apenas na área de TI e chegou a outras, como a de Recursos Humanos, e ao financeiro, que também teve de entender sobre a legislação e suas implicações, como multas.

"Isso trouxe um impulso para a segurança e para a necessidade de essa área ser vista como investimento e não como custo", reforça. Para atender a essa demanda de empresas interessadas em se adequar à LGPD, a Embratel lançou a consultoria Quick Assessment para mapeamento e avaliação dos dados disponíveis, criando um diagnóstico sobre os procedimentos a serem adotados.

Segurança cibernética e proteção de dados são prioridades para a Huawei que,

"Focamos em quase uma dezena de verticais"

Marcelo Motta
Diretor de Cibersegurança e Soluções da Huawei para a América Latina

globalmente, investiu mais de US$ 1 bilhão nesse mercado. "Atuamos no mercado de empresas e focamos em quase uma dezena de verticais", afirma Marcelo Motta, diretor de Cibersegurança e Soluções da Huawei para a América Latina.

Ele concorda que durante a pandemia, a quantidade de acessos remotos cresceu exponencialmente, aumentando riscos e as preocupações com ameaças e ataques cibernéticos. Com isso, passaram a se tornar demandas crescentes a proteção dos sistemas corporativos, autenticação dinâmica e multifatores de usuários, além de segmentação e acesso remoto restrito a aplicações críticas.

A empresa tem um sistema de governança fim a fim, com múltiplos procedimentos de testes e verificações antes de lançamento de produtos no mercado, que também cobre a cadeia de suprimentos e logística. O foco da empresa é na parte de infraestrutura de TIC, mas Motta salienta que o espaço cibernético é muito mais vasto do que o mercado de infraestrutura, o que leva a companhia a trabalhar com ecossistemas para agregar mais valor à conectividade e integrar de forma segura as aplicações de terceiros.

FRAGILIDADE CORPORATIVA

"90% das companhias não possuem nem mesmo ferramentas para gestão de identidade", observa Sergio Ferreira, diretor de produtos da Iteris.

A forte movimentação em torno dos temas pandemia e LGPD impulsionou o mercado de consultorias e empresas de segurança. A Iteris — consultoria de TI com perfil butique — é um dos exemplos, que viu sua receita crescer 38% no ano passado e atingir faturamento de R$ 100 milhões, e com previsão de se aproximar de R$ 150 milhões este ano.

Sergio Ferreira, diretor de produtos da empresa, comenta que os ataques às empresas passaram a ser feitos por organizações criminosas, com uma atuação sofisticada e cirúrgica. Na outra ponta, ele considera que o nível de maturidade de segurança nas empresas ainda não é alto, o que dificulta a situação. "90% das companhias não possuem nem mesmo ferramentas para gestão de identidade", observa.

Mas ele concorda que a pandemia vem ajudando o mundo corporativo a acelerar o processo de transformação digital e, por tabela, mais preocupadas com o ambiente de segurança.

"90% das companhias não possuem nem mesmo ferramentas para gestão de identidade"

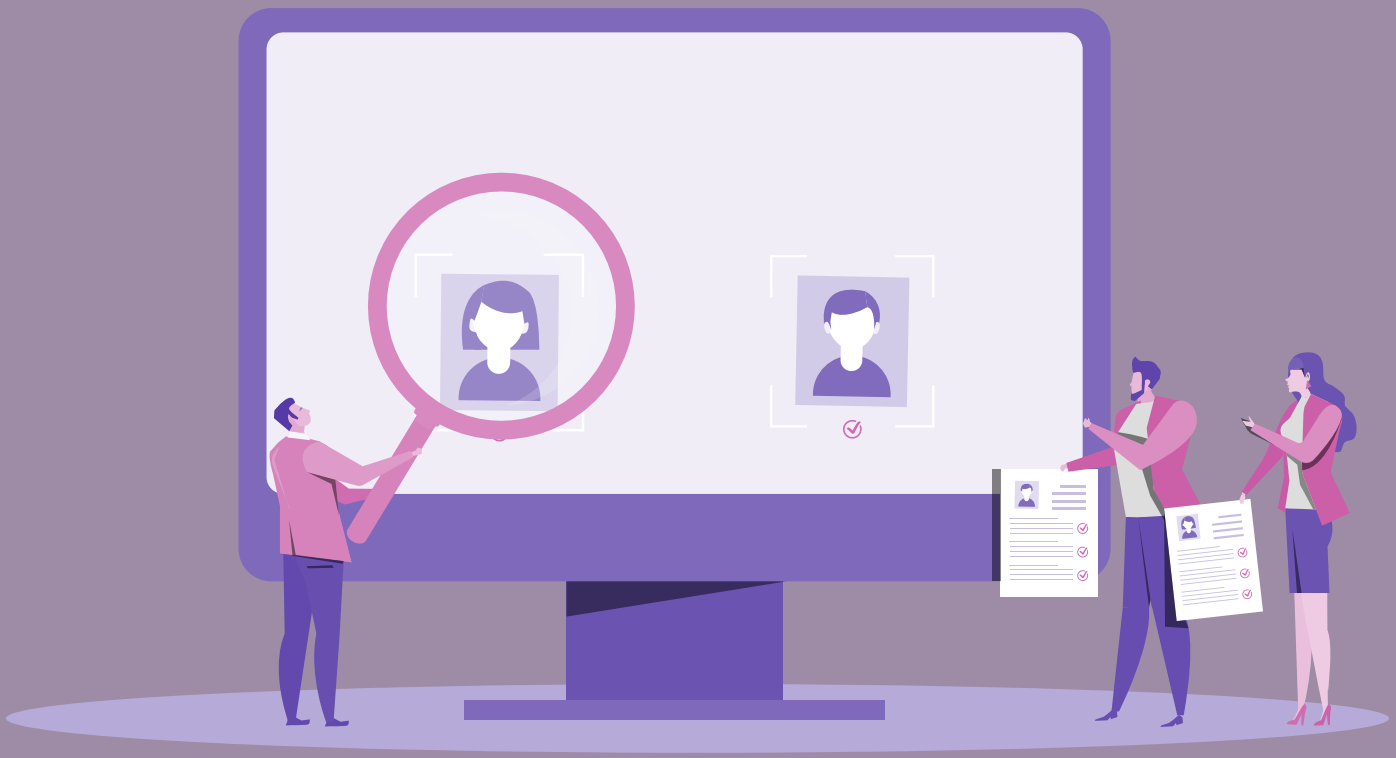
Sergio Ferreira
Diretor de produtos da Iteris

Um rigoroso processo de identificação é um dos pontos do conceito de Zero Trust, abordado por Ferreira. Mas ele enfatiza que também estão dentro desse pacote outras disciplinas, como gestão dos dados, das aplicações, das APIs, que precisam ser acompanhados.

A Iteris aplica o Zero Trust em sua nova definição. Lançado em 2010 pela Forrest Research, o conceito era baseado em "Confie, mas verifique". Com o passar dos anos, a frase que passou a definir esse método é "Nunca confie, sempre verifique".

O executivo acredita que a LGPD deverá ser um estímulo para a propagação de soluções baseadas em Zero Trust. "Hoje não se sabe direito quem acessa as informações. Teremos os primeiros problemas com empresas que terão seus dados vazados e, então, haverá uma corrida para garantir sistemas eficientes de gestão de identificação", prevê.

A consultoria se considera preparada para expandir ainda mais com a evolução desse mercado. Ela possui, por exemplo, um sistema que toma conta da identidade dos usuários. "Se alguém entra de férias, bloqueamos imediatamente todos os acessos. Se é transferido de departamento, bloqueamos o acesso anterior", afirma.



MAMBU

Um nova abordagem para a criação de produtos financeiros integrados.

Experimente a arquitetura baseada em componentes com a plataforma de Core Bancário SaaS da Mambu.

Saiba mais

Siga-nos