mesa-redonda

patrocínio

BioCatch

A BATALHA CONTRA AS FRAUDES DIGITAIS

mesa-redonda

patrocínio

BioCatch

Em seu desafio constante de inovar em produtos, serviços e modelos de negócios, assim como experiências de clientes, os executivos de TI precisam de soluções cada vez mais sofisticadas e inteligentes de segurança. Na chamada terceira plataforma, baseada nos dispositivos móveis, nas redes sociais e no acesso à nuvem, a tecnologia se tornou mais rápida, escalável e acessível, não só para grandes e pequenas empresas, mas também para as pessoas. E isso torna as soluções cada vez mais vulneráveis.

A democratização das transações financeiras, potencializada pela pandemia de coronavírus e pela adoção de soluções já consagradas como o pix e o open finance, produz um inevitável impacto em todo o ecossistema de prevenção de fraudes: a profusão e a diversificação dos golpes financeiros cada vez mais sofisticados exigem soluções eficientes para garantir a integridade das empresas e a confiança dos seus clientes.

Nesta mesa-redonda, realizada em formato híbrido (presencial e remoto), executivos de TI falaram sobre como protegem os sistemas core e atendem a demanda por inovação, para melhor contemplar os novos negócios. E trataram ainda de temas como a conscientização dos usuários, a prevenção contra contas laranjas, a proteção de clientes vulneráveis, os motores de risco, as ferramentas de verificação de identidade e autenticação.

Participaram do debate, coordenado pelo publisher do Informática Hoje, Wilson Moherdaui: **Alex** Amorim, gerente sênior de segurança da informação da Claro; **Fabiano** Rustice, CIO da Pefisa/Pernambucanas; **Lia** Pilatti Machado, gerente executiva de tecnologia e inovação do Banco do Brasil; Marcos **Sirelli**, diretor de TI da Porto; **Pedro** Nuno Trindade dos Santos, gerente executivo de segurança da informação do Banco BMG; Ricardo **Leocádio**, CISO do Banco Mercantil; e **Rogério** Mignella, head de prevenção a fraudes do Banco Original.

Reprodução

“Aqui no banco, temos investido bastante em comunicação, no desenvolvimento de modelos, considerando algoritmos de Inteligência Artificial, para proteger os clientes acima de tudo deles mesmos”.

Lia, do Banco do Brasil

INFORMÁTICA HOJE – A democratização do acesso às transações financeiras tem como um dos efeitos colaterais perversos o fato de facilitar também o acesso dos criminosos a elas. Por isso, as soluções de segurança precisam ser cada vez mais inteligentes, criativas e eficazes. Hoje já são quase 130 milhões de usuários e 450 milhões de chaves de Pix registradas no Brasil. Lia, eu queria que você nos falasse dos desafios que vocês têm encontrado aí no Banco do Brasil, que tem uma vasta capilaridade no país.

LIA – Eu venho trabalhando aqui no banco desde 2006 nesse mundo de prevenção às fraudes em canais eletrônicos, cartões de crédito, etc. Como vocês devem saber, só em 2020 aumentou em 200% o número de golpes de engenharia social. Recentemente ressurgiram alguns golpes que já estavam em baixa, como o golpe do motoboy. Se percebe alguns clientes entregando o cartão ou o celular para um falso entregador ou mesmo sendo envolvidos por falsas centrais. Mas eu queria trazer para o debate um ponto em que eu acredito muito, que é a conscientização. E vou aqui fazer uma analogia: no passado, nós andávamos de carro sem cinto de segurança. Não existia cinto de segurança nos carros. Depois de várias campanhas de conscientização e alterações de legislação, hoje a primeira coisa que fazemos ao entrar no carro é colocar o cinto de segurança. A gente precisaria investir nessa

mesa-
redonda

mesma estratégia para o mundo de segurança digital. O digital chegou muito rápido para todos os cidadãos, mas a educação sobre como se comportar, como navegar, como dirigir na estrada digital não vieram junto. Por isso, nós aqui no banco temos investido bastante em comunicação, no desenvolvimento de modelos, considerando algoritmos de Inteligência Artificial, para proteger os clientes acima de tudo deles mesmos.

IH – Fabiano, você trafega por dois ambientes, do varejo, tanto físico quanto online, das Pernambucanas, e o financeiro, da fintech Pefisa. Quais são suas dores de cabeça mais sérias?

FABIANO – O desafio é exatamente por essa situação peculiar como financeira e de estar servindo ao varejo, não só das Pernambucanas, mas de outros parceiros também. É o desafio do equilíbrio entre a segurança embutida nas funcionalidades e nos serviços financeiros que a gente fornece por meio dos diversos canais, e a experiência. A experiência é fundamental para que a gente garanta que o cliente consiga fazer sua compra, seja de serviços ou produtos. Concordo com a Lia em que a educação é fundamental. Esse trabalho de educação, de inclusão tecnológica e de experiência digital, que têm sido feitos ao longo dos anos, têm que ser aplicados nos aspectos de segurança, proteção de dados e privacidade. No nosso caso aqui, procuramos sempre associar a esse tipo de educação uma forma de manter a experiência mais fluida, para que a fricção seja a menor possível, sempre privilegiando a experiência. Porque, no final das contas, o diferencial competitivo está na experiência. Porque hoje os serviços financeiros estão

Reprodução

“Hoje, os serviços financeiros estão disponíveis tanto nos bancos tradicionais quanto nos digitais, ainda mais considerando a democratização promovida pelo Banco Central, por meio de iniciativas como o Pix e o open banking. Então, o diferencial é a experiência”.

Fabiano, da Pefisa/ Pernambucanas

disponíveis tanto nos bancos tradicionais quanto nos digitais, ainda mais considerando a democratização promovida pelo Banco Central, por meio de iniciativas como o Pix e o open banking. Então, o diferencial é a experiência. Mas essa fluidez da experiência cobra seu preço na hora de decidirmos o que deve ser mais ou menos restritivo.

IH – Nesse sentido, é importante o depoimento do Rogério, do Original, um banco nativo digital. Vocês têm enfrentado muito problema com as chamadas contas laranjas?

ROGÉRIO – Acho que essa é uma dor que todo mundo sofre, não só os bancos digitais como também os bancos tradicionais. O Banco Original tem como seus pilares a segurança, a inovação, a tecnologia, para trazer essas pessoas com segurança para o jogo da bancarização. E aí o nosso grande desafio é conseguir fazer com que os dados fornecidos nesse onboarding sejam validados através de vários birôs. Aí colocamos arcabouços de biometria facial e de consultas externas. Mas sem esquecer o desafio da manutenção da privacidade de dados. Nós temos grandes desafios de autenticação. Como enchemos nossos apps de autenticação biométrica, fatores múltiplos de autenticação, hoje é fundamental trazer a parte mais vulnerável, que é o cliente, para o mundo da segurança. É fazê-lo entender que nenhum banco pede senha, nenhum banco pede uma transação.

IH – É mais difícil para vocês por serem um banco nativo digital?

ROGÉRIO – Particularmente não, porque o banco digital tem essa inovação na veia, na sua estrutura.

mesa-redonda

IH – No caso da Porto, a variedade de fraudes que vocês precisam combater deve ser muito grande, não é Sirelli?

SIRELLI – De fato, seguro é uma avaliação constante de riscos e quando falamos em segurança tem muito a ver com risco. Só para fazer aqui uma conexão com o que a Lia comentou sobre educação, acho que precisamos, sim, abordar essa questão sob a ótica da educação e da cultura, e passar principalmente por entender os benefícios de se ter um processo mais seguro. As pessoas vão ter mais resistências ou até ser mais suscetíveis aos fraudadores enquanto não entenderem o benefício de se utilizar um sistema seguro. Isso vale para questões de tecnologia e vale para experiências físicas inclusive.
Na Porto, nós já temos vários casos associados a riscos de fraudes, tanto em seguros quanto nos produtos financeiros, como cartão e consórcio. Esses são obviamente mais suscetíveis, até pela questão do processo e de atrativos para os fraudadores. Estamos falando diretamente de dinheiro. Mas historicamente há vários tipos de situações que tivemos com relação a fraudes: fraudes de seguros associadas a tentativas de segurar um bem que não necessariamente é aquele. Historicamente a concessão de crédito passa por algo similar. Como é que a gente sabe se o crédito para determinada pessoa pode ser concedido? E aí tem processos, tem tecnologia e tem uma margem de risco que você vai assumir. O Wilson falou aqui de Pix, do open finance e de toda a bancarização que aconteceu, mas a pandemia, sem dúvida, trouxe um universo enorme de pessoas para o mundo digital, sem o devido conhecimento. Na nossa visão, esse aumento na utilização do mundo digital vem acompanhado de uma regulamentação mais completa. A LGPD é uma delas, ao obrigar as empresas a se regular em termos de processos, de tecnologia e educação. E, com o uso de Inteligência Artificial, você consegue identificar mudanças de comportamento e não necessariamente o evento em si, por exemplo, com geolocalização. Se eu sei que uma pessoa tem um hábito de consumo em determinada região, se isso muda, gera um alerta, embora não necessariamente uma trava. A Inteligência Artificial também auxilia na identificação dos dispositivos, que várias empresas já fazem há algum tempo.
Se você rotineiramente utiliza determinado dispositivo, isso gera um rating de utilização. Por último, acho que o desafio que se apresenta para todos aqui é a questão da conexão: com o open finance, você tem uma conectividade entre as empresas que expõe o risco do setor. Antes, muitas operações estavam mais restritas à empresa na relação com o seu cliente, e com os seus parceiros. Agora, esse mercado está mais conectado. A preocupação de todos nós é garantir toda essa operação funcionando de forma conectada e segura. E para isso não acredito que seja apenas atendendo às demandas legais. Acho que a gente vai ter que desenvolver mecanismos de trabalho mútuo para prevenir fraudes e identificação dos processos que estão sendo tratados em cada empresa, de modo que o segmento consiga evitar esses tipos de fraude.

Roberto Assem

“Além do Pix e do open finance, a pandemia, sem dúvida, trouxe um universo enorme de pessoas para o mundo digital, sem o devido conhecimento”.

Sirelli, da Porto

IH – Pedro, o que tira o seu sono diante de fraudes digitais tão sofisticadas?

PEDRO – Embora já tenha sido bastante falado aqui, acho que o pilar dos bancos, além da oferta de soluções (é claro que a gente precisa sobreviver), são produtos com segurança e confiabilidade. Pode até mudar o modus

operandi, mas são sempre os mesmos tipos de abordagem. Eu procuro diferenciar fraudes processuais de ciberfraudes. A gente vê muitas empresas fazendo teste de phishing com os colaboradores, que são bastante efetivos em alguns casos, mas que em outros mostra a grande fragilidade interna da instituição. Daí a importância da conscientização e da educação de todos os tipos de classes de clientes, desde os mais vulneráveis até os mais novos.
Respondendo à sua pergunta, o que mais me tira o sono hoje é quando a gente vai falar de security by design, concepção do produto com segurança. Apesar de falarmos a mesma coisa durante 30 anos, nós continuamos gerando produtos e soluções em que a segurança só é envolvida no final. Não quero generalizar aqui porque isso depende da maturidade e do grau de importância que isso tem para cada instituição. Em muitos casos, precisamos entregar alguma solução ou algum produto, mas a gente não tem um processo, ou tem e não segue um processo adequado de modelagem a ameaças, para tentar identificar todos os quesitos de vulnerabilidades e evitar uma fraude. É o que eu chamo de ciberfraude, que é onde se explora uma vulnerabilidade e não o comportamento do cliente. Acredito que ainda temos que evoluir muito em motores de risco com Inteligência Artificial. Evitar aqueles motores de risco baseados em regras. Regras são muito manuais, muito operacionais, não envolvem um pensamento crítico.

LEOCÁDIO – Acredito que nós estamos em mais um momento histórico digital. Talvez a pergunta certa seja: eu tenho medo ou estou transformando o medo em fobia? Porque são coisas diferentes. As redes sociais e a disseminação da informação têm potencializado nossos medos a ponto de transformá-los em fobia, e isso às vezes me assusta. Temos que entender que o crime sempre esteve na humanidade. No decorrer de sua evolução a humanidade criou meios mais eficazes não propriamente de coibir o crime, mas sim de proteger a vítima de oferecer-se ao criminoso. Então, a questão do aculturamento e do tratamento começa com a personificação e o amadurecimento dos nossos clientes. Mas nós passamos por um problema de identidade, porque, diferentemente de outras modalidades de crimes, uma instituição financeira comentar abertamente para a sociedade sobre fraudes pode transparecer uma fragilidade. E é isso que a gente não quer no nosso ambiente. Então, como chegar ao nosso cliente final sem transparecer que existe uma fragilidade? O Pedro lembrou muito bem que hoje temos fraudes de uma modalidade cibernética. Hoje existe um processo tecnológico totalmente novo, desconhecido e potencializado, porque ele pode ser global; o meu atacante não é mais regional, de uma cidade. Então, nesse novo modelo digital, os nossos modelos de segurança tradicionais não se aplicam mais. Novos modelos têm que surgir. No dia a dia, a gente precisa efetivamente melhorar os nossos controles. O banco Mercantil é um banco de 79 anos. A gente tem feito aqui essa fase de transformação e estamos nos deparando justamente com esse novo momento de fraude. Posso ter jovens talvez muito high techs, mas também tenho muitos clientes que a gente chama de 50+, que não são nativos digitais. Então eles têm uma credibilidade cultural de telefone, que é no que eles acreditam. Conscientizar essas pessoas não é um trabalho simples.

Reprodução

“Acredito que ainda temos que evoluir muito em motores de risco com Inteligência Artificial. Evitar aqueles motores de risco baseados em regras. Regras são muito manuais, muito operacionais, não envolvem um pensamento crítico”.

Pedro, do BMG

mesa-redonda

patrocínio

BioCatch

IH – Esse ponto em que o Leocádio tocou é muito importante: como não demonstrar para o cliente a fragilidade do banco. Esse é um grande dilema. Porque, na medida em que você evita mostrar para o cliente que tem algumas fragilidades, você acaba expondo o cliente a essas fragilidades. E os bancos, em geral, evitam demonstrar fragilidades, porque isso pode gerar uma perda de confiança do cliente no banco. Como vocês reagem diante desse dilema? [

LIA – Essa é uma ótima pergunta. O desafio é fazermos uma comunicação e uma abordagem leves para não provocar pânico nos clientes. Temos investido em algumas soluções, tipo a comunicação via push, em que a gente fala para o cliente: "Foi você quem fez essa transação?" Se foi o cliente, a gente libera aquela transação e eventualmente, se tiver realizado algum bloqueio de senha ou de cartão, nós já fazemos os desbloqueios. E se o cliente diz que não foi ele, a gente encaminha outra mensagem e tenta acolher, dar o tratamento adequado para ele naquele momento. O grande desafio é mesmo experiência versus segurança. O nosso desafio agora é tratar em 10 segundos uma transação de Pix e negar ou não negar. O Pix trouxe um ensinamento bastante grande para a gente: o de que temos que investir cada vez mais em modelos de IA, para poder atuar no tempo das novas formas de transação. E a forma de comunicação com o cliente é importantíssima. Quando a gente pergunta se foi ele que tentou liberar um dispositivo, não digo para ele que tem um problema, mas eu o alerto de que pode estar acontecendo alguma coisa estranha no acesso à conta dele. Por isso, precisamos investir bastante e cada vez mais em IA, em biometria, seja comportamental, seja facial, de voz, o que for.

Reprodução

"Nesse novo modelo digital, os nossos modelos de segurança tradicionais não se aplicam mais. Novos modelos têm que surgir. No dia a dia, a gente precisa efetivamente melhorar os nossos controles".

Leocádio, do Banco Mercantil

ALEX – A legislação já indica há algum tempo a importância de as instituições financeiras terem muito claro o plano de ciber-resiliência. Quando a gente olha para o modelo bancarizado, há o Banco Central, uma autarquia muito forte, agora há também a ANPD (Autoridade Nacional de Proteção de Dados), com o surgimento da LGPD, que começa a ter força. No Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados, que é uma ONG, a gente percebe falta de comunicação clara de muitas instituições financeiras, como forma de preservar sua imagem. Falta transparência.

SIRELLI – Sua pergunta é bastante interessante. Acho que essa é uma questão fundamental, porque a todo momento que surge um golpe, parece que acontece uma inversão de valores. A culpa parece recair 100% sobre a instituição, porque ela não tomou todos os cuidados necessários. Mas nem sempre isso é verdade. Existe até um certo glamour em relação aos golpes bem-sucedidos. Parece que é uma questão intelectualmente valorizada. Como a gente faz para colocar as coisas nos devidos lugares? Quem é o criminoso nesse processo? Pela dificuldade de identificação, a responsabilidade passa automaticamente a ser das instituições. Legalmente todas as instituições têm obrigações. Não se trata de comunicar o que está acontecendo, isso não se discute. Mas acho que é uma questão que precisamos inverter. Afinal, quando há um problema desse tipo, todo mundo do setor precisa se apoiar, para evitar que isso aconteça novamente, porque no final da linha isso encarece o custo final para a sociedade. Aí, as empresas não se expõem da maneira que

deveriam até legalmente, justamente para não deixar transparecer essa vulnerabilidade, o que acaba por deixar o fraudador numa posição mais protegida. É péssimo isso!

ROGÉRIO – Não é só o custo exponencial, mas também a experiência dos bons clientes acaba sendo prejudicada, porque as instituições financeiras colocam mais e mais ferramentas, mais e mais autenticações. E com isso, o cliente que toma todos os cuidados acaba sendo prejudicado na sua experiência. Nós, instituições financeiras, somos muito colaborativos, mas não podemos oferecer uma experiência melhor para o cliente em detrimento da segurança.

IH – Alex, como o smartphone é o grande responsável por essa democratização da conectividade, conta como as operadoras lidam com as soluções de prevenção às fraudes, tanto em relação a elas próprias, quanto aos seus clientes usuários da operadora.

ALEX – Essa questão da interconexão da experiência do cliente com a segurança é um grande desafio. Quando se trata de fraudes, existem basicamente três momentos: o momento do onboard do cliente, quando ele está entrando na plataforma; o momento de alteração de dados que ele pode fazer, como uma troca de endereço ou de número de celular; e por fim tem o momento da transação. É nesses três momentos que podem acontecer as fraudes. A Claro, além de fazer parte desse ecossistema, também tem um banco digital, o Claro Pay, que tem todas essas dores das instituições financeiras. Como o Rogério comentou, é muito importante entender como funciona essa composição do nível de segurança versus a necessidade transacional.

Roberto Assem

“A primeira sugestão para os vendors é não querer vender uma bala de prata. Isso não existe. Não faz sentido achar que determinado produto vai resolver todos os nossos problemas. É preciso ter muita transparência na relação de parceria”.

Alex, da Claro

Então, é fundamental entender qual é o meio que está sendo usado para a validação do cliente. Estamos usando, como é muito comum, somente um SMS? Será que estamos olhando para toda a jornada? Estamos usando biometria? Estamos considerando documentoscopia? Então, acho que o grande ponto é entender que as operadoras são apenas meios que fazem parte desse ecossistema. Quando a gente olha para o mundo das operadoras, tem fraude para todo lado!

IH – A chegada da 5G vai potencializar ainda mais os riscos de fraude?

ALEX – Esse ponto é muito importante. O usuário vai ter o acesso de forma mais veloz. Mas a grande preocupação é com para a Internet das Coisas (IoT), pois vem a possibilidade de colocar um chip em qualquer coisa. A minha geladeira vai falar diretamente com a internet. Não vou mais ter aquele modem, que de certa forma fazia o papel de firewall, que tinha algumas devidas proteções by default. Será que ao introduzirmos a IoT, vamos fazer o hardening adequado? O usuário vai estar atento a isso? Quando começamos a ter camadas de segurança adicionais no usuário e ele começa a ter mais poder, independente do lugar onde esteja, a gente se pergunta: qual é o nível de segurança que eu estou colocando nesse endpoint, nesse meu usuário? Isso acaba se ampliando muito agora, no mundo da IoT. As coisas vão se desdobrando a partir de um ponto único que começa a mudar essa perspectiva de uma segurança centralizada para esse modelo do ZTNA - Zero Trust Network Access, em que a gente começa a entrar agora.

SIRELLI – Eu queria complementar a questão da 5G. O Alex é o especialista aqui nesse assunto, mas eu queria apontar uma vantagem da 5G: o avanço da tecnologia na latência e na capacidade de transmissão também possibilita outras camadas de segurança que hoje a tecnologia 4G não permite. Então, no fundo, vai haver um trade off interessante: vai haver realmente um aumento de dispositivos IoT, mas também serão implementados outros mecanismos de segurança pela nova tecnologia, talvez até aumentando a segurança no final.

mesa-redonda

IH – Eu queria saber de vocês se existem mecanismos específicos de proteção aos clientes vulneráveis. Os bancos tradicionais devem enfrentar esse problema com mais frequência. Já os digitais e as fintechs, menos, porque lidam com um público mais jovem e mais antenado.

LIA – Aqui no Banco do Brasil, temos uma política específica para cuidar dos vulneráveis, não só dos idosos, mas daqueles que por alguma razão não estão habituados ao mundo digital. Recentemente criamos até um modelo para a identificação de clientes vulneráveis. A gente tem inclusive ajustado alguns scripts de central de atendimento para esse grupo. Nós temos feito uma abordagem bastante específica, para não criar barreiras para a pessoa transacionar, até porque existem nesse grupo diferentes níveis de conhecimento do digital e da abordagem dos fraudadores.

PEDRO – Acho que esse público precisa realmente, de um tratamento especial. Mas, só por curiosidade: nos testes que fazemos de phishing para clientes, o público vulnerável não é o que cai mais. Por incrível que pareça, são os médios. Parece que uma parte do público vulnerável tem mais cuidado ao tratar os seus valores. Não estou generalizando, estou me baseando em números. A gente sabe quando se trata de uma pessoa vulnerável, que necessita um pouco mais de atenção. E esse acompanhamento, que é ligar, entender e dar suporte, faz uma diferença enorme. Além disso, o que tem resultado muito positivo é o básico bem-feito, que é sempre comunicar, avisar, seja por e-mail ou ligação, ou até mesmo por SMS. Esse processo de conscientização é fundamental.

LEOCÁDIO – No Mercantil, esse talvez seja o nosso maior desafio. Será que nós estamos no caminho certo? É a pergunta que me faço todos os dias. Será que não deveríamos criar commodities de segurança? Hoje eu posso escolher um carro que já vem de fábrica com seguro, com airbag, e outros itens de segurança. Mesmo que o meu avô inicialmente não saiba dirigir aquele carro, com o tempo ele passa a lidar com o câmbio automático, com o vidro elétrico e com aquilo que pode trazer proteção para ele. Ele não precisa se preocupar em aprender, porque se trata de uma commodity de segurança do carro. É lógico que isso tem um custo agregado. E eu posso até oferecer a ele um carro blindado, se isso estiver no meu portfólio de produtos. Da mesma forma, a gente pode oferecer um produto financeiro melhor para o meu avô, desde que ele receba um mínimo de educação para recebê-lo. E isso pode ser, para nós do sistema financeiro, um atrativo de negócio. Nós que somos de segurança também temos que pensar em negócios.

Roberto Assem

“Como enchemos nossos apps de autenticação biométrica, fatores múltiplos de autenticação, hoje é fundamental trazer a parte mais vulnerável, que é o cliente, para o mundo da segurança”.

Rogério, do Banco Original

IH – Como vocês têm usado a Inteligência Artificial para fazer análises preditivas e, de alguma forma, se antecipar aos problemas de segurança na interação com os clientes de vocês?

FABIANO – Na verdade, a gente usa aqui ferramentas de mercado que são tradicionalmente baseadas em modelagens estatísticas, utilizando modelos de machine learning e Inteligência Artificial. As ferramentas antifraudes tradicionais, sejam para fraude transacional, de cartão de crédito ou de contas, e também fraudes de subscrição e em processos de alterações cadastrais e de invasão de conta, já embarcam há algum tempo as tecnologias de IA. Adicionalmente nós desenvolvemos internamente – porque procuramos a solução no mercado e não encontramos – uma solução própria de documentoscopia, a análise da autenticidade de documentos, utilizando basicamente redes neurais e modelos de machine learning. Eu queria acrescentar que, embora já tenha sido um pilar importante para a segurança, estamos chegando à triste conclusão de que a biometria facial não tem muito futuro, pelos recentes problemas que vários provedores têm enfrentado recentemente. É claro que se tem buscado sempre evoluir,

mesa-
redonda

patrocínio

mas temos buscado outras alternativas. Ela continua sendo um componente dentro do processo de autenticação do cliente, mas deixará de ser um pilar. Isso porque, do mesmo jeito que a IA trabalha a nosso favor, também trabalha contra. Vejam, por exemplo, a utilização da IA para o deepfake.

ROGÉRIO – Como um banco inovador, o Banco Original usa a IA tanto na identificação e na autenticidade do documento, quanto na experiência do cliente, ao conseguir trocar seu dado cadastral, ou também na identificação de devices, de troca de senha, de redes de acesso, e da geolocalização. E tudo isso se junta no motor de prevenção às fraudes, que a gente usa bastante para prevenir e garantir a autenticidade das transações.

FABIANO – A gente aqui sofre muito com o SIM-Swap. Nós temos estudado soluções em para validar a idade ou o tempo de ativação do chip. Sem dúvida, isso ajuda. Mas o SIM-Swap é hoje um dos pilares de autenticação, principalmente para os bancos digitais e para o cliente. Então precisamos trabalhar forte nesse aspecto também e imagino que as operadoras estejam olhando para isso.

ALEX – O SIM-Swap não é exclusivo de uma operadora, é de todas. Hoje existem crimes muito bem organizados fazendo isso. A própria Anatel tem perguntado o que nós temos feito em relação a isso. Mas esse é um dos indicadores que tem caído muito. Porém, quando acontece, é um barulho muito grande, especialmente quando atinge aquele usuário que tem milhões de seguidores. O que acontece muito, não é o hacker que acessou e fez o SIM-Swap. É muito mais a fraude baseada no legítimo uso: são pessoas autorizadas, que têm o cadastro na empresa, que estão usando o equipamento da empresa. É uma situação em que a gente passa a olhar mais para o lado comportamental. É tudo aquilo básico: tem uma senha forte? Tem um segundo fator de autenticação? Tem uma biometria? A questão é como otimizar tudo isso. E pensando que são pessoas autorizadas, que fazem parte do seu dia a dia e que de fato têm autorização para fazer isso. É por isso que a fraude entra em um nível tão qualificado, que o grande objetivo é olhar não mais o mato alto, mas aquele desvio de comportamento padrão.

IH – Para terminar, gostaria de saber o que vocês esperam dos fornecedores de tecnologia quando se trata de soluções de segurança?

PEDRO – Da mesma forma que hoje é inadmissível comprar um carro sem cinto de segurança, é inadmissível a gente receber um produto sem segurança. Então, no mínimo, os fornecedores de segurança têm que estar mais alinhados ao negócio. Em resumo, os fornecedores precisam melhorar o alinhamento entre o negócio e as soluções de segurança.

LIA – De forma bem resumida, espero dos fornecedores produtos que não alterem a experiência do cliente e que consigam agregar segurança, mas de forma transparente. Quanto mais transparente for a segurança para o usuário, melhor.

LEOCÁDIO – Eu espero que os fornecedores não se tornem o meu ponto de comprometimento de risco.

FABIANO – Os provedores de segurança devem sim levar em consideração os aspectos que foram discutidos aqui: acima de tudo, o básico, a garantia de integridade, mas levando em consideração a importância da experiência. De alguma forma, tem que se buscar, trabalhar, pesquisar e prover soluções que nos permitam trazer esse equilíbrio entre a segurança e a experiência.

SIRELLI – A pergunta é ótima. Um dos aspectos que eu gostaria de salientar é o modelo de negócio. Tenho me deparado com muitas soluções de segurança que não fazem sentido para as empresas do ponto de vista de garantia de compra futura, em um volume determinado que a gente tem que definir antes da compra. Então acho que o modelo de negócio precisa ser muito aderente ao que as empresas precisam. E por uso, por consumo e no modelo de serviço em nuvem. O outro aspecto é uma simplificação, não empilhando soluções. É trazer soluções mais simples do ponto de vista de como plugar isso nos nossos negócios. Acho que a gente foi criando soluções e hoje elas estão empilhadas. Por último, a questão da disponibilidade é fundamental. Ela se tornou um fator crítico nos processos.

ROGÉRIO – Acho que se trata sobretudo de garantir o básico alinhado a essa nova tendência de fraudes. Se é biometria facial, que ela garanta a autenticação com isso e que, como o Leocádio comentou, não se torne um problema para a gente.

ALEX – A primeira sugestão para os vendors é não querer vender uma bala de prata. Isso não existe. Não faz sentido achar que determinado produto vai resolver todos os nossos problemas. É preciso ter muita transparência na relação de parceria. Outro ponto é: para quem já tem as soluções, ajudar a utilizá-las melhor. Muitas vezes a gente acaba comprando uma solução, sem dar a atenção necessária para a melhor forma de utilizá-la.