Fraudes feitas por funcionários: o crime nasce na empresa

Rita D'Andrea (*)

Uma empresa de serviços digitais descobriu, recentemente, que era vítima de fraudes perpetradas por seus próprios funcionários

Profissionais internos renovavam continuamente pacotes de degustação de serviços oferecidos gratuitamente a vários clientes. Dessa forma, alguns usuários tinham acesso pleno à oferta desta empresa sem, no entanto, pagar um centavo por isso.

Parceiros externos desta corporação também estavam envolvidos no golpe. O quadro de fraudes era agravado, ainda, pelo fato de ocorrer constantemente o roubo ou a compra de senhas de acesso às aplicações de negócios desta empresa – os sistemas que, ativados, autorizariam a entrega dos serviços digitais. Uma investigação policial mostrou, posteriormente, que essas ações criminosas eram provocadas por pressões e ameaças de traficantes aos operadores do contact center desta empresa.

Em plena era de transformação digital, cada etapa desta fraude ocorreu por meio do uso indevido das aplicações corporativas, sistemas responsáveis por manter os processos e os negócios dessa corporação funcionando. Ao final do dia, milhões de reais se perderam, e essa empresa teve de iniciar uma revolução interna e externa para garantir a segurança de seus processos e aplicações.

A fraude ocupacional, também conhecida como desfalque, ocorre quando, por meio de um processo deliberado, um colaborador faz mau uso ou emprega mal os recursos ou o patrimônio de uma empresa em seu próprio benefício pessoal. Segundo a empresa de pesquisas de mercado Static Brain, em 2014 funcionários norte-americanos roubaram US$ 50 milhões das empresas onde trabalham.

Um dado preocupante é que esse ataque interno é difícil de ser descoberto: o tempo médio de ocorrência da fraude antes de sua detecção é de 2 anos.

Em 2014, dados do Estudo Global de Fraudes (um levantamento realizado pela maior entidade de fiscais de fraudes dos EUA, a Association of Certified Fraud Examiners), mostraram que 77% das fraudes ocupacionais foram cometidas por funcionários das áreas de contabilidade, operações, vendas, gestão executiva, atendimento ao cliente, compras ou finanças. Quanto aos setores da economia, bancos e serviços financeiros, governo e administração pública, telecomunicações e indústria tenderam a ter o maior número de casos de fraude. Somente no mercado norte-americano de Telecom, por exemplo, estima-se que as fraudes tragam prejuízos anuais de mais de US$ 40 bilhões por ano (dado da Communications Fraud Control Association).

A fraude ocorre primariamente em empresas com claras vulnerabilidades em seus processos e sistemas. São corporações que já vivem a transformação digital, mas ainda não contam com políticas e tecnologias de segurança à altura da engenhosidade dos criminosos. Neste quadro, os sistemas de faturamento (entre outras aplicações de negócios) e as vulnerabilidades das redes são facilmente explorados para obter acesso. Uma das fraudes mais comuns é o roubo de identidades – somente este tipo de crime gerou, nos EUA, no ano passado, perdas na ordem de US$ 4,32 bilhões.

O roubo de identidade é especialmente eficaz na hora do criminoso acessar os dados essenciais para que se cometa o desfalque.

Complexas aplicações corporativas rodando na nuvem ou fora da nuvem são o alvo preferencial: usuários internos irão disparar ações que estão além de sua área de trabalho e dos direitos de acesso que receberam de seu empregador, passando a autorizar, de forma fraudulenta, a compra ou venda de serviços, o cadastramento de novos clientes, a transferência de recursos, etc.

A luta contra esse tipo de fraude é algo que alia soluções tecnológicas a novos processos, treinamentos e controles (foco em pessoas). Algumas das melhores práticas para reduzir o risco de fraudes incluem estabelecer uma central de atendimento antifraude pronta a receber denúncias (anônimas ou não). É importante, ainda, efetuar auditorias de surpresa.

Nesta empreitada é fundamental, ainda, implementar sistemas que monitorem e analisem ativamente os dados e as aplicações da empresa. Esses sistemas "lerão" o comportamento da aplicação e emitirão um alerta no caso de acessos estranhos ocorrerem. A plataforma IAM (Identity and Access Management, gerenciamento de identidade e acesso) pode ajudar nesta luta. Essa tecnologia de segurança autentica com grande precisão a identidade (e os consequentes direitos de acesso) da pessoa que deseja interagir com a aplicação missão crítica.

As soluções IAM são um aliado importante do CISO na defesa dos sistemas que mantém o negócio funcionando – não por acaso, os mesmos sistemas que o fraudador tenta penetrar.

Uma das missões dessas soluções é analisar o contexto de onde está sendo feito o acesso do usuário. Onde ele está? Por qual tipo de dispositivo a pessoa está acessando a aplicação? O acesso está sendo feito no horário comercial? Esse usuário passou pelo crivo da tecnologia MFA (Multiple Factor Authentication, autenticação realizada a partir de múltiplos fatores – senha, reconhecimento biométrico, posse de um token)? É recomendável que o uso de soluções como estas esteja inserido num quadro de ações que visem a transformação da cultura corporativa e a interiorização, por parte dos funcionários, de novos valores.

A checagem de cada um desses pontos aumenta a inviolabilidade do ambiente corporativo e dificulta a realização das fraudes. Em tempos de transformação digital, derrota a fraude quem, entre várias iniciativas, protege o coração do negócio: a aplicação.

(*) É country manager da F5 Brasil.

IoT: criando uma nova geração de equipamentos para salvar vidas

O setor da saúde destaca-se por sua vocação pelo uso de novas soluções tecnológicas

Rodrigo Moreni (*)

Embora o cenário ainda não seja perfeito, há uma grande receptividade para novidades como IoT (Intenet of Things= Internet das coisas) que vem tendo sua aplicação ampliada. Responsável por conectar à internet dispositivos eletrônicos, equipamentos médicos e sistemas, tanto aqueles diretamente envolvidos no cuidado ao paciente, como na gestão das instituições de saúde, a IoT tem um potencial de utilização gigantesco. Dados do Boston Technology Corporation (BTC) mostram que as aplicações desta revolucionária tecnologia no setor da saúde devem, até 2020, crescer $ 117 bilhões.

Os usuários por sua vez, parecem estar mais abertos à internet das coisas. O que até pouco tempo atrás era visto como um bicho de sete cabeças, com o surgimento da mobilidade e das redes sociais passou a ter maior aceitação. Com a modernização das tecnologias e as interfaces mais amigáveis e recursos como touch screen, as pessoas passaram a transferir sua experiência do pessoal para o profissional. Isso tudo abriu espaço para o desenvolvimento de outras tecnologias, como de equipamentos médicos.

Além disso, segundo a consultoria Grand View Research, o mercado global de saúde investiu em 2014 US$ 58,9 bilhões em dispositivos, software e serviços de IoT. E esse montante deve atingir US$ 410 bilhões até em 2022. E não é de hoje que a indústria investe no desenvolvimento de componentes eletrônicos, software, sensores de conectividade, alarmes, avançados sistemas de controle, entre outros facilitadores, que são cada vez mais incorporados em equipamentos médicos e laboratoriais das mais diversas naturezas.

Na indústria de equipamentos médicos Fanem, por exemplo, começamos monitorando a temperatura de nossas câmaras de conservação imunobiológicos e hematológicos e substituindo os controles em papel por relatórios eletrônicos. Aos poucos evoluímos, incluindo outros parâmetros, capazes de controlar tudo à distância, através da nuvem. E hoje, as câmaras fabricadas em nosso parque industrial, 100% nacional, dispõem de conexões wi-fi, ethernet e bluetooth e monitoram indicadores, inclusive por dispositivos móveis. Assim é possível saber como estão as temperaturas no interior das câmaras, quantas vezes foram abertas as portas, as condições do sistema elétrico e do consumo de energia, entre outros.

Partindo daí, a ideia é que a capacidade de monitorar e de analisar os dados vindos dos equipamentos estenda-se para outras áreas. Desde equipamentos simples como um banho-maria até os mais avançados de suporte a vida. O padrão HL7, que se refere a um conjunto de normas internacionais para a representação e a transferência de dados clínicos e administrativos entre sistemas de informação em saúde, já está sendo inserido em diversos equipamentos. Esse protocolo aplicado em uma incubadora para tratamento de recém-nascidos, de maneira análoga, permite que o equipamento comunique-se com o prontuário eletrônico do paciente (PEP) e, com isso, informações sobre os parâmetros do bebê, quadro clínico e terapia possam ser cruzadas.

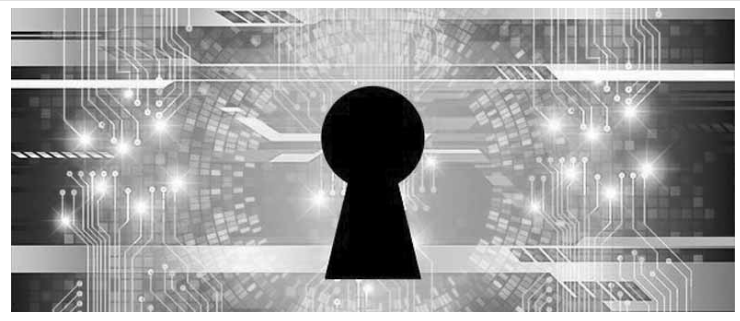
Estes dados, separadamente, parecem não fazer sentido, mas podem ser utilizados pelos fabricantes visando aprimorar equipamentos; pelos usuários para aplicar melhores cuidados; e até pela instituição de saúde, como uma ferramenta importante para melhorar a administração de recursos e fazer a gestão técnica e financeira de todo o processo. Nada pode ser ignorado, pois em conjunto, tornam-se informações valiosas que permitem em um contexto mais amplo inclusive saber como anda a saúde de uma população. E é exatamente esse tipo de aplicação que vai aumentar ainda mais a relevância da IoT.

Por outro lado, por mais que a indústria médica aposte em tecnologia de ponta para o desenvolvimento de novos produtos, o fato dos processos de certificação serem muito custosos e longos, aumenta a cautela, e às vezes até inviabiliza a adoção de algumas tecnologias, especialmente em equipamentos de suporte a vida. Por isso, a evolução muitas vezes parece ser lenta e menos visível.

No entanto, sem dúvida nenhuma a IoT cumpre seu papel e ajuda a equilibrar custos com qualidade e eficácia de atendimento, proporcionando uma visão geral do cenário e contribuindo para uma mudança na saúde como um todo. Quanto menores forem as barreiras para a indústria, mais tecnologias estiverem conectadas, maior for o número de equipamentos que conversarem entre si, maiores serão as chances de avançarmos na qualidade dos cuidados despendidos com a saúde.

(*) É chefe do departamento de projetos do laboratório da Fanem.

A América Latina e sua posição na cibersegurança global



Quando se trata de tendências de cibersegurança, são muitos os problemas semelhantes em diferentes partes do mundo. Do Canadá ao Japão, as discussões sobre cibersegurança giram em torno de desafios parecidas, e na América Latina não é muito diferente. Mas, como em quase todas as situações, existem particularidades que são únicas de cada contexto. A inteligência de ameaças do FortiGuard Labs apresenta algumas tendências que as empresas da América Latina e do Caribe devem levar em conta para evitar ciberataques maciços aos seus negócios, incluindo estratégias e tecnologias de adaptação.

Infraestrutura de segurança atualizada

O primeiro padrão observado nos dados estatísticos da região está relacionado à vida ativa das ameaças conhecidas como malware. A persistência das ciberameaças na América Latina confirma a necessidade urgente de implementar soluções tecnológicas avançadas, considerando a atividade significativa das ameaças presentes no mercado há anos. Um exemplo é o Shellshock, um malware que ainda é uma ameaça significativa na região, apesar de ter surgido há vários anos. Isso mostra como a infraestrutura de computadores está muitas vezes desatualizada ou sem correções, deixando-a vulnerável mesmo a ataques mais antigos.

Outra ameaça menos conhecida, mas ainda dominante, na América Latina se refere aos ataques por meio de websites. Na verdade, os ataques atuais são feitos usando o Muieblackcat, uma ferramenta ucraniana projetada para detectar vulnerabilidades. Esta ferramenta, que utiliza a linguagem de programação PHP, procura por websites vulneráveis e, por meio deles, dispara ataques a alvos específicos.

É importante notar que há muitos ataques na região que usam a linguagem PHP; isso significa que muitos servidores usam essa tecnologia. Esses websites, além de estarem infectados, também podem infectar os visitantes. Os provedores de serviços e os profissionais de TI devem pensar duas vezes antes de usar o código PHP e devem garantir que estão totalmente atualizados, ao passo que os clientes também devem procurar obter as configurações de segurança adequadas para se protegerem.

O atraso tecnológico ou a falta de atualizações do sistema e correções de segurança levam a uma maior vulnerabilidade, não só a novas ameaças, mas também a ataques mais antigos que continuam aproveitando essas lacunas.

Dispositivos móveis com sistema Android

A ameaça aos dispositivos móveis é real. Se você considerar a região da América Latina e do Caribe, três dos dez ataques de malware mais difundidos e detectados estão em dispositivos móveis Android. Esta não era a realidade há um ano, ou mesmo há 10 meses, mas em janeiro deste ano, a tecnologia móvel já representava mais da metade das detecções de malware no Caribe. Estamos vendo uma mudança rápida no cenário de ameaças à cibersegurança, e esta é uma tendência que não vai desaparecer tão rápido. Começamos a discutir sobre essas ameaças há sete anos, e logo elas se tornarão uma preocupação ainda maior, passando à frente de outras prioridades.

Do total de malwares em dispositivos móveis detectados na América Latina e no Caribe no primeiro trimestre de 2017, 28% deles são malwares para dispositivos Android, mostrando um crescimento mais rápido do que em outras regiões em comparação ao percentual anterior de 20% no último trimestre de 2016.

Escassez de profissionais de cibersegurança

Um problema global é a falta de profissionais e especialistas em segurança da computação. Somente nos Estados Unidos, existem cerca de 200.000 vagas de emprego para profissionais de cibersegurança. Este é um número muito alto e um problema global ainda maior, também evidente na América Latina e no Caribe.

As empresas encontram dificuldade para manter um departamento de TI grande o suficiente para proteger seus sistemas, redes e clientes diante de uma lacuna significativa entre os profissionais do setor e a falta de qualificação necessária. A falta de treinamento neste setor complicado tem consequências graves que podem custar a credibilidade da empresa. É por isso que hoje, mais do que nunca, devemos apoiar e capacitar programas de treinamento para instruir e especializar adequadamente os profissionais da região.

Não é surpresa alguma que a América Latina ainda tenha um longo caminho a percorrer em sua preparação para cibersegurança, principalmente quando comparada a outras regiões do mundo. Porém, as empresas e organizações podem começar a se proteger destas ameaças, atualizando seus sistemas, investindo ainda mais em seus departamentos de TI e adotando novas soluções tecnológicas que oferecem visibilidade e gerenciamento amplos, poderosos e automatizados.

A estratégia fundamental que todos os executivos devem seguir na abordagem às ameaças de cibersegurança começa com o conhecimento do inimigo – a detecção é necessária para a prevenção. Ao implementar soluções de tecnologia avançada, as empresas podem saber antecipadamente quais ameaças estão em suas redes e dispositivos, permitindo ações proativas para garantir dados confidenciais e de clientes não corrompidos ou afetados por esses ataques. Caso contrário, as empresas se tornam alvos abertos, podendo ser a próxima vítima de cibercriminosos.

(Fonte: Derek Manky, estrategista de segurança global da Fortinet).

News @TI

Startup de educação atinge 50 milhões de faturamento em 2017

@2017 é um ano de comemoração para a Quero Educação. Empresa líder em tecnologia de marketing educacional no Brasil, a startup, que faturava R$ 5 milhões em 2015, está fechando seu ano fiscal com um faturamento de R$ 50 milhões. No primeiros semestre, a empresa ofereceu mais de 760 mil bolsas de estudo, com descontos de até 70%, em parceria com mais de 1000 faculdades de todo o País, e já ultrapassa mais de mais de 60 mil alunos matriculados.