Como proteger a rede da empresa sem interferir na mobilidade dos colaboradores?

Por Bill Hogan (*)

Os profissionais de segurança de TI de grandes empresas em todas as indústrias enfrentam a tarefa diária de ter que proteger uma superfície de ataque em expansão

Os pontos vulneráveis de entrada costumavam estar dentro dos muros da organização, onde firewalls e ferramentas de segurança on-line podiam protegê-los, mas as redes agora se tornaram um ambiente sem fronteiras, em constante evolução, graças ao uso de nuvem, a Internet das coisas (IoT) e uma força de trabalho cada vez mais móvel.

Os avanços tecnológicos, combinados com uma onda de funcionários digitalmente inteligentes inundando o local de trabalho, levaram mais pessoas a trabalhar de suas casas ou outros locais fora do escritório. Além disso, trabalhar em uma variedade cada vez mais diversificada de dispositivos. E, embora possa ser uma surpresa, esse aumento na força de trabalho móvel tornou-se comum mesmo nas indústrias mais altamente regulamentadas.

De acordo com um estudo recente, 65% das organizações permitem a conexão de dispositivos pessoais às redes corporativas. Na América Latina e no Caribe, estima-se que o número de empregos móveis foi de 740.000 em 2016, com outros 980 mil empregos indiretamente suportados por tecnologias móveis.

Em todos os setores, as empresas estão adotando os esquemas de trabalho móvel devido aos seus vários benefícios de redução de custos, aumento da produtividade e eficiência dos funcionários e maior retenção de colaboradores. Mas estes esquemas também envolvem riscos ao permitir que dispositivos e aplicativos não gerenciados pelas organizações, acessem suas redes corporativas e seus recursos digitais.

A segurança da rede continua sendo uma prioridade. 95% dos CIOs relatam sua preocupação com os e-mails armazenados em dispositivos pessoais e 94% deles se preocupam com informações corporativas armazenadas em aplicativos móveis. O objetivo das empresas é encontrar um equilíbrio entre o benefício do BYOD e BYOA e a mitigação dos fatores de risco à cibersegurança.

Problemas de segurança em ambientes móveis

Para se beneficiar das capacidades do trabalho móvel sem comprometer a segurança da rede ou perder a visibilidade do uso de dados classificados, as organizações devem considerar três aspectos principais:

• Shadow IT

Políticas rigorosas sobre aplicativos e serviços que os funcionários estão autorizados a usar em seus dispositivos podem fazer com que os funcionários contornem este protocolo de segurança para adquirir soluções que os ajudarão a tornar seu trabalho mais eficiente. Isso pode ser um grande risco à segurança, já que as equipes de TI não conseguem proteger dados em aplicativos que não conhecem, e nem podem garantir que esses aplicativos serão atualizados com as correções mais recentes. E se esses dados forem violados, é improvável que as equipes de TI percebam isso e consigam implementar protocolos adequados de resposta a incidentes.

• Vazamento de dados

O vazamento de dados se refere ao fluxo não autorizado de dados corporativos do datacenter seguro para um dispositivo ou local não autorizado. Isso geralmente ocorre quando os funcionários transferem arquivos entre dispositivos corporativos e pessoais ou quando funcionários não relacionados têm acesso a dados privilegiados. Com o uso cada vez mais comum de ambientes na nuvem e de aplicativos SaaS, e o número maior de dispositivos de usuários conectados, as equipes de TI geralmente perdem visibilidade do uso e fluxo dos dados.

• Segurança de aplicativos

Com a mobilidade laboral, surge um número cada vez maior de aplicativos, independentemente de estarem sendo usados nos negócios ou não. Em média, as organizações têm 216 aplicativos executados em sua organização, sem falar nos aplicativos pessoais armazenados nos dispositivos dos funcionários. Quando esses dispositivos de usuários e aplicativos se conectam à rede, é necessária uma segurança forte para o aplicativo. Isto é válido principalmente para aplicativos na nuvem, onde pode ser difícil para as equipes de TI aplicar as políticas de segurança padrão de suas organizações.

Em resumo

Para aproveitar ao máximo os benefícios da força de trabalho móvel que faz uso de seus dispositivos pessoais, as organizações precisam implementar controles de segurança adicionais que protejam e monitorem os dados sem serem muito rigorosos, pois isso pode inibir a mobilidade. As equipes de TI devem adotar uma abordagem em camadas para a segurança, fornecendo visibilidade do fluxo dos dados em toda a rede. Especificamente, este protocolo de segurança deve oferecer segurança de aplicativos, segurança de dispositivos de usuários, segmentação de rede e segurança dos ambientes na nuvem, além de defesas no perímetro da rede padrão. Tudo isso em um quadro de segurança integrado e abrangente, poderoso e automatizado para poder responder às ameaças atuais e futuras.

(*) É vice-presidente da Fortinet.

A Internet das Coisas exigirá uma nova abordagem na segurança corporativa

A transformação digital que vem acontecendo nos últimos anos permitiu que muitas empresas fossem criadas e se tornassem bem sucedidas em um curto período, mas com ela também vieram novas vulnerabilidades que ameaçam a segurança dos dados e, consequentemente, a continuidade dos negócios

José Matias Neto (*)

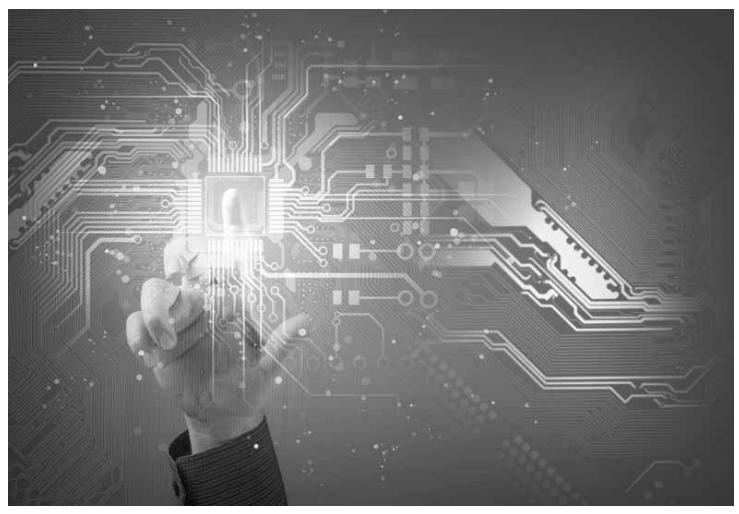
Tecnologias como a computação em nuvem e os aplicativos móveis ampliam as fronteiras da rede e multiplicam por cinco a possível superfície de ataque. Fatores como a imensa quantidade de dados gerados, a diversidade de pessoas que se conectam à rede corporativa, a variedade de dispositivos para gerenciar, tanto os próprios como os de terceiros, formam um cenário complexo que deve ser administrado pelas equipes de segurança, na maioria das vezes, com mão de obra limitada e orçamentos estáveis.

Uma grande preocupação dos gestores é como usufruir dos benefícios gerados pela Internet das Coisas sem colocar os dados corporativos em risco. Considerando que o custo dos sensores caiu pela metade nos últimos 10 anos e os custos da computação e da banda de Internet ficaram 60 vezes e 40 vezes mais baratos, respectivamente, podemos esperar um aumento incrível de novos dispositivos no mercado.

Atualmente, estima-se que há 50 bilhões de dispositivos conectados que produzem 44 ZB (zettabytes) de dados, cerca de 1 trilhão de gigabytes. Mas há ainda 15 bilhões de dispositivos que poderiam, mas ainda não estão conectados. Bilhões de novos dispositivos conectados significam bilhões de novas possibilidades de ataques cibernéticos.

Os dispositivos IoT são feitos de uma série cada vez maior de blocos de construção de software e hardware, levando a uma complexidade significativa, que é inimiga da segurança. Tudo indica que esses dispositivos não estão preparados para lidar com o desafio da segurança atual.

Muitos dos fornecedores de dispositivos como câmeras, medidores elétricos, eletrodomésticos, sensores, drones, etc, não consideram a segurança como um fator crítico no processo de criação de seus produtos, o que pode trazer muitos problemas aos seus usuários. Ataques contra os dispositivos IoT já estão acontecendo com frequência, como em câmeras IP com controles de segurança fracos, medidores inteligentes com falhas básicas de criptografia, dispositivos de saúde ou dispositivos SCADA (usado em usinas nucleares) que alimentam infraestrutura crítica em todo o mundo, entre outros.



Assim como já aconteceu com os dispositivos móveis como smartphones e tablets, é inútil tentar barrar a inserção de dispositivos IoT no ambiente corporativo, eles precisam ser integrados ao ambiente, mas de forma segura.

Para se preparar para essa transformação é preciso mudar totalmente a forma como pensamos e lidamos com a segurança. As empresas devem adotar uma visão onipresente de segurança da informação, que deve estar inserida em suas culturas, de maneira que a segurança sempre acompanhe o crescimento dos negócios, sem interrupção e que proteja a empresa contra fraudes, perda de propriedade intelectual e contra as ameaças à privacidade.

Com o gigantesco volume de dados e dispositivos para gerenciar, não é possível esperar que o trabalho continue sendo feito manualmente. Automação e integração são dois conceitos que devem crescer cada vez mais na segurança da informação e no combate ao cibercrime. Soluções integradas que trocam informações entre si e eliminam brechas de comunicação, assim como soluções mais inteligentes, capazes de avaliar e reconhecer ameaças em frações de segundo, serão grandes aliadas para aumentar a velocidade na análise de dados e no bloqueio às ameaças.

A segurança da informação não é mais uma batalha a ser vencida, nem sequer uma guerra, pois o trabalho não acaba mesmo depois de uma vitória. A segurança é uma evolução constante. Os responsáveis pela gestão corporativa precisam entender que a segurança cibernética é um componente de missão crítica para sua estratégia de negócio.

(*) É diretor de suporte técnico da McAfee para América Latina .

Mais um ano termina e a profecia sobre o fim dos cartões de plástico não se cumpre

Nos últimos tempos, em praticamente todas as semanas nos deparamos com manchetes como: "Fintech X testa pagamentos com relógios, óculos, pulseiras, canetas, anéis, self, sorrisos etc". Normalmente essas chamadas são acompanhadas de análises do tipo: "Em pouco tempo os cartões de crédito em formato plástico como o conhecemos deixarão de existir". Ocorre que estamos chegando ao final de mais um ano e isto parece longe de acontecer.

Ao contrário disso, se fizermos um teste e colocarmos no serviço de busca do Google a frase: "Fintech lança cartão", nos surpreenderemos com a quantidade de reportagens que demonstram que, apesar de profetizarem o fim do cartão plástico, esses próprios inovadores não abrem mão de terem suas marcas devidamente impressas e materializadas em pequenos pedaços de plástico guardadas nas carteiras de seus clientes.

Parece incoerente, mas é a realidade. Mesmo adotando um discurso exterior de que o plástico está ultrapassado, na hora de garantir a sustentabilidade do negócio, financeiramente falando, ninguém abre mão do plástico. E por quê? Porque, queiram ou não queiram admitir, ele é, e acredito que ainda será por muito tempo, a melhor alternativa para garantir pagamentos ágeis, massificados e seguros do mundo.

Tem sido assim no mundo todo. Por mais e maiores novidades tecnológicas que apareçam, os pedidos para a impressão de cartões plásticos continuam aumentando, a pedido das maiores e mais tradicionais marcas da indústria financeira do planeta e também das mais novas e disruptivas startups financeiras.

Não que se neguem as possibilidades e os ganhos que possam representar as novas mídias, como o telefone celular e a infinidade de variáveis trazidas pela Internet das Coisas, mas quando falamos de cartões de crédito, estamos falando de dinheiro. E quando se fala de dinheiro há que se levar em consideração um fator primordial que é a segurança.

Desde a invenção do chip nunca se ouvir falar de uma quebra se quer da criptografia existente neste tipo de sistema que pudesse resultar em fraudes. Os vazamentos que acontecem nunca estão ligados à quebra dos padrões de segurança dos cartões com chip propriamente ditos. Essas falhas acontecem em outras fases do processamento das transações. E são justamente estas etapas vulneráveis que ficam expostas quando se abandona o cartão de plástico para escolher um celular, um par de óculos, uma pulseira, um relógio ou qualquer outro objeto.

Já faz pelo menos uma década que se profetiza a massificação dos pagamentos por celular, por exemplo, mas ainda são muito poucos os projetos neste sentido que conseguiram um nível de massificação que possa ser comparável à escalabilidade possibilitada pelos cartões de plástico.

Além da questão da segurança, existe a própria questão da universalidade da tecnologia. Quantas pessoas atualmente tem condições de ter um relógio dotado da tecnologia que permite fazer pagamentos? E anéis ? E pulseiras?

Quantos estabelecimentos comerciais e prestadores de serviço atualmente estão preparados para receber pagamentos inovadores como estes? Quanto será preciso ser investido para que esta receptividade passe a estar presente em todo território nacional, por exemplo? E como ficará esta questão nos países subdesenvolvidos e em desenvolvimento?

Por esses e outros motivos, apesar de toda a onda disruptiva e modernizante que inunda o noticiário, é preciso que alguém se lance contra a correnteza para dizer o contrário: "O cartão de crédito de plástico não está perto de ser extinto e muito provavelmente nunca será".

(Fonte: Daniel Lecuona é CEO da G&L Cards and Payments).

News @TI

Aprenda a desenvolver apps para plataforma iOS nas próximas férias de janeiro

@Com a proposta de ensinar programação para adultos que conhecem e desconhecem sobre tecnologia, a Quaddro Treinamentos – maior centro de ensino mobile do Brasil – tem inicio a 5° turma do curso "Swift – Intensivo de Férias", desenvolvido para quem deseja entrar no mundo mobile. As aulas acontecem no período de 8 de janeiro a 2 de fevereiro de 2018, de segunda à sexta, das 9h às 18h. No total são 152 horas de curso + 8 horas de curso on-line de Lógica de Programação. No curso, os alunos aprendem realmente a programar e já criam alguns apps durante o treinamento. As vagas são limitadas e os pré-requisitos solicitados são apenas conhecimentos básicos em Mac OS e Lógica de Programação. As inscrições podem ser feitas no site (http://www.quaddro.com.br/).