F5 Networks lista principais batalhas de segurança em 2016

Em um mundo cada vez mais conectado, data centers serão derrubados por causa da vulnerabilidade de dispositivos Internet das Coisas (IoT), o tráfego criptografado SSL continuará a esconder ataques e planos de "Disaster Recovery" poderão preservar os processos das empresas

A F5 Networks, líder em soluções de ADN (Application Delivery Networking) tecnologia que garante a entrega de aplicações rodando em ambiente Web – apresenta suas previsões sobre as mais importantes batalhas de segurança em 2016:

Falhas de segurança de dispositivos da Internet das Coisas (IoT) irão afetar grandes data centers

À medida que mais dispositivos e aplicativos se unem ao ecossistema IoT, a probabilidade de vulnerabilidades originárias do IoT chegarem a afetar os data centers aumenta exponencialmente. Assim, em 2016, a luta passará para outro front: manter o tráfego IoT seguro e afastado de áreas sensíveis – especialmente dos data centers.

Apps de pagamento serão um grande alvo dos hackers

Se 2015 testemunhou grandes ataques a dados corporativos, em 2016 os hackers voltarão sua atenção às vulnerabilidades de apps para pagamento a partir de dispositivos móveis. É imperativo que os desenvolvedores de apps para pagamento móvel – desde instituições financeiras até empresas independentes – adotem em todo o processo de trabalho soluções de segurança eficazes e ágeis, capazes de repelir os inevitáveis ataques.

Em 2016, o SSL estará em toda parte

2016 será o ano em que a criptografia SSL se tornará padrão. Com essa mudança, será mais difícil para as equipes de segurança identificar (visualizar) e rastrear perdas de dados. Em meados de 2015, por exemplo, hackers obtiveram as impressões digitais e os números da seguridade social de mais de 22 milhões de norte-americanos na invasão ao Office of Personnel Management. A ação passou despercebida durante muitos meses porque não havia um protocolo para inspeção do tráfego de saída criptografado – tráfego que continha os dados roubados. As atuais ferramentas de segurança monitoram, tipicamente, a existência de malware no tráfego entrante. Infelizmente o modelo *zero-trust/SSL everywhere* traz um ponto cego para a inspeção do fluxo de saída. A necessidade de 'analisar e inspecionar' o tráfego de saída será crucial para a segurança da rede em 2016.

A nuvem híbrida finalmente será padrão de mercado

Embora se venha falando na nuvem há anos e as empresas venham lentamente movendo dados e serviços para fora de suas instalações próprias, 2016 será o ano em que as empresas aceitarão que a nuvem híbrida é o novo padrão do mercado. Quer seja uma combinação de armazenamento local e na nuvem, quer seja o uso de serviços baseados na nuvem, ou até mesmo a Shadow IT migrando para a nuvem corporativa, a nuvem já está na sua empresa e veio para ficar. O desafio dos gestores de TIC será aprender como monitorar e administrar todas as instâncias da nuvem híbrida, assegurando que dados e aplicativos críticos estejam sempre disponíveis e seguros.

Hackers selecionarão alvos e contornarão soluções tradicionais de segurança

A próxima onda de ataques cibernéticos segue evoluindo e os hackers estão se movendo em direção a uma seleção de alvos mais definidos – para isso, alguns cibercriminosos estão escrevendo códigos para contornar tecnologias de alguns fornecedores de segurança. O resultado desta estratégia serão mutações do malware a uma velocidade difícil de acompanhar. Em 2016, as empresas lutarão para antecipar ameaças de rápida transformação e em constante evolução. Para isso, usarão soluções de análise comportamental, uma nova forma de assegurar que os dados e aplicativos estejam fazendo aquilo para que foram criados.

Disaster Recovery garantirá continuidade de negócios em caso de ataques

Embora as empresas movam cada vez mais seus dados para a nuvem, muitas delas ainda estão fazendo backup em seu próprio data center. A redundância é a sua política de segurança e, no caso de um provedor de nuvem ficar indisponível, espera-se que garanta a continuidade dos negócios. Com roubos de dados e ataques cibernéticos em ascensão, as empresas estão na corda bamba e a nuvem é uma das principais preocupações quanto à segurança. Os principais provedores de serviços de nuvem não foram hackeados ainda, mas as corporações usuárias precisam estar preparadas. É por isso que 2016 será o ano do planejamento de recuperação de desastres (Disaster Recovery) na nuvem.

Grandes alianças entre fornecedores de segurança surgirão em 2016

Já vimos o início deste movimento mas, em 2016, haverá uma tendência de aumento das alianças entre fornecedores tradicionais de segurança, empresas de redes e provedores de nuvem. Na era dos data centers híbridos e ambientes de trabalho móveis, as empresas não podem mais depender de firewalls de rede tradicionais para manter seus dados seguros; fornecedores atuando em áreas tecnológicas específicas precisarão de ajuda de outras empresas para fechar as lacunas de seus portfólios. O objetivo de todos será criar uma solução de segurança mais abrangente. O perímetro tradicional está desaparecendo e os fornecedores estão juntando esforços para

proporcionar segurança à camada de aplicação, onde quer que ela esteja sendo processada, qualquer que seja o dispositivo pelo qual seja acessada.

Sobre a F5 Networks

A F5 Networks provê soluções para o universo das aplicações. A F5 Networks ajuda as organizações a criarem soluções escaláveis de computação em nuvem, data center e SDN (Software Defined Network, rede definida por software). Em todos os casos, a tecnologia F5 Networks garante a entrega das aplicações a qualquer usuário, em qualquer lugar, a qualquer momento. A plataforma F5 amplia o alcance das soluções de TI – isso é feito com a ajuda de um rico ecossistema de parceiros da F5 Networks, incluindo fornecedores de soluções para orquestração de data centers. Um dos destaques da estratégia de negócios da F5 Networks é sua flexibilidade, permitindo que os usuários projetem o modelo de infraestrutura que melhor atenda às suas necessidades. As maiores empresas globais confiam na F5 Networks para estar à frente das tendências de computação em nuvem, segurança e mobilidade. A companhia, que tem sede em Seattle, Estados Unidos, atua no mercado brasileiro desde 2001, através de distribuidores e revendas. No final de 2005, a F5 instalou oficialmente sua subsidiária brasileira, em São Paulo.

Mais informações: www.f5networks.com