Por Maurício Bandeira (*)

Como nos últimos anos, 2017 promete ser um ano de grandes inovações tecnológicas. E, para fazer frente a tantas novidades, é necessário redobrar os cuidados no que se refere à cibersegurança, pois os hackers tentarão manipular dados, criando dúvidas quanto à autenticidade da informação e, assim, prejudicando a tomada de decisões, tanto no setor público, quanto no privado.

A compreensão dos riscos cibernéticos existentes e emergentes é mais relevante do que nunca, pois afetam a segurança internacional, a política e a estabilidade econômica. Apesar do surgimento de novas startups para desenvolver soluções em segurança, evitar possíveis ataques virtuais também exige empenho do governo, mídia e líderes empresariais. No entanto, os ataques cibernéticos têm sido tão frequentes e as táticas evoluem tão rapidamente que já ultrapassaram os mecanismos de defesa implementados há pouco tempo.

Ataques cibernéticos recentes envolveram a exclusão de dados de grandes empresas, a edição de manchetes de notícias e a interrupção do acesso à informação. A temporada de eleições nos EUA foi prejudicada pela inundação de “notícias falsas” que, segundo pesquisadores independentes, foi afetada por meio de uma sofisticada campanha que criou e espalhou artigos falsos por meio de botnets – que são redes de computadores infectadas por bots semelhantes, programas fabricados para automatizar procedimentos, geralmente repetitivos.

Em 2017, será ainda mais difícil para indivíduos e organizações confiar em informações, dados e notícias, pois os ataques à integridade de dados podem ter repercussão ainda maior do que manchetes de notícias falsas. A alteração da pontuação dos cartões de crédito ou dos números das contas bancárias poderá ser uma consequência bastante comum caso as empresas não se protejam contra os possíveis ataques.

Até mesmo um concorrente corporativo que queira obter vantagem competitiva pode alterar as bases de dados de contas financeiras para distorcer a realidade, imediatamente antes do fechamento de um contrato significativo. As organizações precisarão aprender rapidamente como se proteger contra sabotagem dos dados, à medida que esse tipo de cibercrime se torna cada vez mais frequente.

Além disso, a previsão é de um aumento de ataques aos dispositivos IoT (Internet das Coisas), que serão aproveitados como botnets e usados como pontos de lançamento para propagação de malware, SPAM, ataques DdoS e anonimização de atividades mal-intencionadas.

Estamos vivendo a Era da Internet das Coisas (IoT), com conexões e controles digitais por todos os lados e ameaças cada vez maiores às empresas e aos governos.

No que diz respeito à espionagem cibernética e à guerra de informação, a previsão é de que violações de segredos de estado continuarão a influenciar a política global e a espionagem afetará até as próximas eleições na América Latina e na Europa. Países como Rússia, China, Irã e Coreia do Norte continuarão a ser regiões de grande preocupação em 2017, à medida que continuam a ser celeiros para o crescimento do cibercrime.

A cada dia, as organizações reforçam suas defesas contra os ataques cibernéticos e, como consequência, os hackers colocarão seu foco no elemento humano, com investidas direcionadas e engenharia social astuta e eficaz, explorando o elo mais fraco das empresas: os colaboradores.

As pressões regulatórias farão com que as empresas sejam obrigadas a desenvolver talentos em segurança cibernética tão bons que sejam capazes de detectar vulnerabilidades em sua rede, sistema e segurança antes mesmo de uma ação efetiva dos criminosos. Provavelmente, os

primeiros centros financeiros com times deste porte estarão em Hong Kong, Cingapura, União Europeia e Estados Unidos.

A indústria de serviços financeiros e outros setores regulados poderão ser os primeiros a adotar a tomada de vigilância em cibersegurança como parte crítica dos processos de fusões e aquisições.

As empresas brasileiras também são alvos constantes de processos de quebra de segurança e ataques cibernéticos. Neste sentido, cresce a importância da contratação de executivos da área de segurança da informação, com boa capacidade em gestão de pessoas e habilidades técnicas na área. Pesquisas mostram que 40% das empresas entendem a segurança como oportunidade de negócio e 71% veem ameaças e riscos da segurança digital como impedimentos para a inovação.

No dia a dia, como usuário da internet, algumas atitudes simples podem evitar um futuro ataque e garantir tanto a sua proteção, quanto a da sua empresa. Já para as empresas, é muito importante desenvolver a conscientização dos funcionários sobre o que é fraude de engenharia social, principalmente, entre os funcionários do departamento financeiro. A discrição nas redes sociais, no que se refere a assuntos relacionados ao trabalho, é sempre o melhor caminho. Além disso, é importante lembrar que o colaborador deve ser cauteloso ao clicar em hyperlinks, verificando sempre a origem e o destino dos mesmos.

A organização também faz parte das atitudes essenciais que um funcionário deve ter para evitar ações de hackers. Manter uma lista de fornecedores pré-aprovados ao conhecimento de todos os envolvidos nas atividades e desenvolver um sistema com senha para verificar a autenticidade de pedidos de transferência eletrônica e a legitimidade de emails e ligações de executivos seniores.

Outras ações importantes que tanto funcionários quanto indivíduos devem ter em seu dia a dia é evitar o compartilhamento excessivo de informação sobre a vida pessoal e descartar informações pessoais de forma segura. Estes conselhos podem parecer simples e batidos, mas a partir destes dados, organizações mal intencionadas podem construir seu perfil e acessar suas informações ou as informações da empresa para a qual você trabalha.

Este ano, veremos uma intensificação das ameaças, além de uma confusão entre o que é responsabilidade do governo, dos mercados, das empresas e da sociedade civil. Vale a pena se antecipar a estes riscos a fim de evitar que o pior aconteça.

(*) **Maurício Bandeira** é gerente de Produtos Financeiros da Aon Brasil.

Fonte: Estadão Política/Blog do Fausto Macedo, em 16.03.2017.