Hackers, traidores e violações de dados na era da dependência cibernética

Por Marcel-Patric Braun (*)

Os negócios de hoje dependem da nuvem. Mas o que o mundo tem chamado de “nuvem” não é realmente uma nuvem. É um símbolo para conexões globais de dados numerosas e complexas demais para serem diagramadas. Enquanto as empresas terceirizam serviços de TI para uma miríade de fornecedores especializados, as conexões se tornam ainda mais nebulosas.

Não são apenas os websites. Telefones, edifícios e carros também se conectam à nuvem. Essa tendência só tende a aumentar à medida em que encontramos outras maneiras para que dispositivos e aparelhos controlados por dados tornem nossa vida mais fácil.

Desde 2009, um poderoso motor de busca, Shodan, tem identificado todos os dispositivos conectados ao redor do mundo. E os hackers tem usado o Shodan para ter acesso a edifícios bancários, salas de conferências, edifícios de apartamentos, hotéis e até à sede australiana do Google.

Na nossa “internet das coisas”, parece que nada na nuvem é perfeitamente seguro e as empresas estão conectados de forma que elas nem percebem. Nem mesmo as empresas que consideramos como bastiões da internet – Google, Apple, eBay – são invencíveis.

O Hacker Criminoso

Na década passada, hackers criminosos enviaram milhares de vírus bem sucedidos, como

cavalos de tróia, malwares e outros códigos maliciosos, para sistemas corporativos, instalações governamentais, computadores pessoais e smartphones. Eles roubam dados de cartões de crédito, projetos da aviação militar, segredos corporativos, identidades de consumidores e muito mais.

Preocupada com o potencial impacto de ataques cibernéticos a infra-estruturas críticas (CI), a Comissão Europeia propôs que todos os operadores de CI publiquem os ataques a seus sistemas em um registro oficial. Isto irá permitir que os governos nacionais monitorem tais ataques e tentem impedir a sua propagação.

Na verdade, a Deutsche Telekom (DT) já instalou armadilhas eletrônicas, chamadas honeypots, ao longo de seus sistemas em todo o mundo. Honeypots atraem hackers aparentando oferecerem dados valiosos. Na realidade, eles estão isolados da rede da empresa. Eles são constantemente monitorados para que as companhias possam registrar e analisar cada ataque e relatá-lo às autoridades. O resultado é surpreendente: a DT registra uma média de 800.000 ataques separados por dia.

Nem todos os ataques acabam em violações. No entanto, de acordo com o relatório cibernético Poneman, da IBM, a cada 2 anos, 22% das empresas sofrem alguma violação de dados com vazamentos de até 100.000 registros cada. Quantas dessas brechas as empresas realmente detectam? Menos de 1%, e quase sempre é tarde demais para evitar a perda de dados.

O Hacker Acidental

Os grandes incidentes de hacking são tão proeminente na mídia que muitas empresas não percebem que os hackers externos só criam 40% das violações. Outros 30% são causados por empregados e contratados. Isso é um percentual considerável!

A negligência é o problema mais comum. Pode ser algo tão simples como um empregado ou consultor que se conecte a um servidor corporativo através de um smartphone que tenha um malware. Com 2 milhões de malwares e aplicações móveis de alto risco, esta é uma ameaça cada vez mais comum. Muitas vezes, a incapacidade de manter os sistemas de TI e software também os deixa expostos a qualquer vírus ou outros códigos maliciosos que vêm junto.

A negligência pode ser difícil de ser controlada em uma nuvem de conexões terceirizadas. As empresas, mesmo as instituições financeiras críticas, tendem a usar uma alta proporção de terceiros para serviços de tecnologia da informação (TI). Como a TI evolui rapidamente, a terceirização permite a flexibilidade de contratação de especialistas, conforme necessário.

O outsourcing de TI conecta empresas primeiro aos contratantes e, em seguida, a subcontratantes não identificados, criando cadeias de risco cibernético “interno”. A subcontratação do e-mail corporativo é muito comum. Um vírus no sistema de email de uma empresa subcontratada pode se espalhar rapidamente para milhares de multinacionais.

Quantas empresas sabem os nomes, muito menos os protocolos de segurança cibernéticos, de todos os seus subcontratados ao redor do mundo? Quantos dispositivos desprotegidos privados estão ligados a empresas subcontratadas, que estão ligadas a terceirizados, que estão ligados a multinacionais? A possibilidade de uma violação negligente cresce a cada conexão.

O Hacker Privilegiado

Um dos desafios internos é a negligência; o outro é o mau uso intencional. O uso interno indevido produz 8% das violações registradas.

A maioria dos hackers externos estão apenas sondando os sistemas da empresa com a esperança de ter sorte. Espiões internos e consultores de TI não precisam ter sorte porque eles sabem exatamente onde encontrar os dados mais valiosos: projetos de produtos inovadores e propriedade intelectual (IP), detalhes sobre pagamentos e bancos e os dados confidenciais de clientes.

Como eles fazem isso? C-suiters com cartões de memória, engenheiros enviando projetos para seus computadores pessoais, administradores de sistema que se passam por outros usuários no sistema, funcionários de call-center que escrevem os números de cartão de crédito do cliente de baixo para cima – os traidores são criativos! Em 70% dos casos, leva dias, semanas, meses ou até anos para as empresas descobrirem os vazamentos.

Espionagem, sabotagem e roubo internos: por que eles fazem isso? 10% simplesmente tem algum ressentimento em relação à empresa, geralmente por terem sido demitidos. Não é nenhuma surpresa que 72% das violações internas tenham sido motivadas por questões financeiras. Funcionários e consultores roubam dados secretos para iniciar suas próprias empresas, para vendê-los a concorrentes ou entregá-los de presente para seus novos empregadores. De fato, 79% dos roubos de IP ocorrem no mês seguinte à saída de um empregado.

O custo do problema

Devido à sua abordagem específica, estas ameaças internas podem desferir um golpe nos resultados da companhia que dura anos. O custo médio de uma violação corporativa é de US$ 3,5 milhões e estes valores podem ser ainda mais altos.

Em 2014, uma única violação ocorrida em 2011 custou à empresa afetada o total de US$ 200 milhões. Uma violação em 2013 deixou expostos os nomes de usuários, senhas e dados de cartões de crédito de 110 milhões de pessoas. Os custos para essa empresa poderão alcançar US$ 1 bilhão. Estas são apenas duas das violações de hackers criminosos que ficam mais caras a cada ano.

Violações internas são mais difíceis de quantificar. Em parte porque elas são embaraçosas e raramente relatadas. É também porque muitas vezes elas dizem respeito ao IP roubado. Quantos negócios exclusivos uma empresa perde quando um único design inovador de produto é roubado? Possivelmente milhões.

Dependência x defesa cibernética

É fácil entender por que o mundo se tornou ciberneticamente dependente. A nuvem torna os negócios globais mais rápidos e fáceis. Infelizmente, assim como cresce nossa dependência cibernética, também se elevam os custos de uma potencial violação de dados. A necessidade de combinar defesas cibernéticas com nossa dependência cibernética torna-se mais urgente a cada dia.

Além de due diligence e melhores protocolos de segurança cibernética, as empresas devem se preparar para o custo de uma violação. Como a maioria delas não consegue reservar US$ 200 milhões para um potencial desastre cibernético, ter um seguro é um fator crítico. No entanto, neste momento, 72% das empresas europeias e 79% das empresas alemãs não têm seguro cibernético, de acordo com a Federação das Associações Europeias de Gestão de Risco (FERMA). Por que isso?

Assim como o risco cibernético, o seguro cibernético também tem sido um tema nebuloso. Inicialmente, as seguradoras eram tão lentas como todos os outros para perceber a dimensão e a urgência do risco cibernético. Isso está mudando.

Apólices para riscos cibernéticos agora incluem não só uma cobertura extensa, mas também apoio de emergência, incluindo telefones de contato disponíveis 24 horas em todo o mundo. Quando a infração ocorre, as seguradoras podem responder imediatamente, conectando empresas de serviços de resposta a violações a taxas preferenciais. Estes incluem: especialistas em computação forense e em gestão de crises, empresas de monitoramento de crédito e identidade, além de assessoria jurídica. A investigação forense é especialmente importantes para a recuperação dos dados roubados.

A cobertura cibernética agora compensa por conta de pesados custos de recuperação de dados, extorsão cibernética, responsabilidade pela segurança e privacidade, resposta a emergências, computação forense, gestão de crises, proteção da reputação, notificação e defesa legal. O seguro de riscos cibernéticos cobre também perdas causadas pela interrupção do negócio e despesas extras que não são cobertas pelo seguro patrimonial.

Como o risco cibernético cruza várias linhas de negócio, o grupo de trabalho de seguros cibernéticos deve incluir especialistas experientes em reivindicações de responsabilidade civil, bens e linhas financeiras. Eles serão capazes de trabalhar lado a lado com os clientes para coordenar uma solução completa para a reivindicação o mais rápido possível. A resposta rápida em caso de sinistro é fundamental para a recuperação das empresas.

Com uma taxa de violações cibernéticas corporativas de 22%, é hora de enfrentar as perdas de resultado que se escondem na nuvem e tomar medidas concretas para se proteger contra elas. Quando a violação ocorrer, parceiros de seguros fortes podem ajudar as empresas a recuperar

os dados, reduzir as perdas, proteger a reputação e retomar o negócio rapidamente.

Checklist do risco cibernético

É certo que o risco virtual é mais complexo do que nunca. Ele tem que ser mapeado e medido com precisão para que as seguradoras sejam capaz de oferecer políticas cibernéticos adequadas.

As empresas devem criar um mapa de risco cibernético, começando com o elo da cadeia mais próximo a elas. Esse elo é um risco interno. Em seguida, elas devem avançar ao longo da sua cadeia de terceiros e subcontratados, inspecionando os protocolos de segurança e nodos de agregação de risco.

Uma vez que todos os riscos possíveis tenham sido mapeados, a probabilidade e o custo de uma violação ou falha no sistema em cada nodo de risco devem ser medidos e um custo deve ser atribuído a ele. A soma de todos esses valores vai determinar a exposição máxima de custos. Este também é um bom momento para rever os riscos. Algum deles pode ser reduzido com a melhora dos sistemas ou a contratação de diferentes fornecedores ou subcontratados?

Em seguida, as empresas devem verificar seus riscos cibernéticos vis a vis suas apólices existentes para bens, responsabilidade civil e de risco reputacional. Existem lacunas de cobertura para interrupção de negócios não-físicos, de terceiros, ou outros riscos? Quanto mais detalhado esse mapa do risco, melhor as seguradoras poderão ajudar a esclarecer se a cobertura existente é suficiente para certos riscos ou se é necessária uma cobertura cibernética.

As empresas podem decidir que elas querem manter o risco até um limite, por isso elas devem definir um máximo dedutível e discuti-lo com as seguradoras.

Com um mapa de risco cibernético consistente e dedutíveis definidos, garantir uma apólice cibernética será então apenas uma questão de adquirir a melhor cobertura pelo preço mais razoável.

(*) **Marcel-Patric Braun** é Chefe de Linhas Financeiras para a Alemanha, Áustria e Europa Oriental do XL Group.

Fonte: IDGNOW! , em 04.03.2015.