Governo dos EUA e empresas pressionam bancas por seguranÃ§a de dados

Grandes clientes corporativos estão exigindo das bancas americanas medidas mais sérias para proteger seus dados “sensíveis” na Internet. Bancos e empresas de grande porte querem que os escritórios de advocacia usem o que há de mais avançado em tecnologia para detectar e deter ataques de *hackers* internacionais, que querem roubar segredos corporativos para uso próprio ou para vender, de acordo com o jornal *New York Times*.

No entanto, as bancas suspeitam que, por trás dessas pressões, estejam os órgãos de segurança dos EUA. Alguns desses órgãos, que espionam governos e corporações estrangeiras, conforme demonstrado pelos documentos divulgados pelo ex-agente da CIA Edward Snowden, sabem que percorrem uma via de duas mãos: *hackers* estrangeiros, privados ou governamentais, podem fazer a mesma coisa.

A pressão das corporações sobre as bancas é nova. Mas a pressão exercida pelos órgãos de segurança, liderada pelo FBI, ocorre desde 2011. Em novembro, agentes do FBI começaram a fazer reuniões com grupos de representantes de escritórios de advocacia, especialmente os que atuam no exterior, para discutir a segurança na Internet e a espionagem corporativa.

Os órgãos de segurança sabem que isso acontece. Em fevereiro, por exemplo, os jornais divulgaram que as comunicações entre os advogados da Mayer Brown, uma banca de Chicago, e autoridades do governo da Indonésia foram interceptadas pela agência de inteligência da Austrália, que tem conexões estreitas com a Agência de Segurança Nacional (NSA – *National Security Agency*) dos EUA, o órgão de espionagem americano que ficou sobre fogo cruzado em todo o mundo depois da divulgação de seus documentos por Snowden.

Segundo o *New York Times*, a vulnerabilidade dos escritórios de advocacia a ataques de *hackers* se tornou uma grande preocupação para as agências de segurança, porque as bancas mantêm um “rico repositório” de segredos corporativos, estratégias empresariais e de propriedade intelectual.

Além disso, há uma grande probabilidade, segundo os órgãos de segurança, de que os *hackers* tenham acesso a informações sobre grandes transações empresariais antes que elas sejam anunciadas, porque toda a documentação essencial está nos sistemas de computação das bancas.

Os órgãos de segurança acreditam que os escritórios não estão se empenhando o suficiente para impedir ataques de *hackers* estrangeiros. Para eles, as bancas constituem o ponto fraco na segurança corporativa dos EUA no que se refere à proteção *online*.

Representantes de grandes bancas disseram, em *off*, ao jornal que a preocupação dos órgãos de segurança é “exagerada”. Para eles, os ataques de *hackers* são predominantemente *phishing* de *e-mails* — uma tentativa de roubar informações pessoais e senhas de contas bancárias e cartões de crédito. Esse é um tipo de ataque, eles dizem, que hoje já é facilmente detectado e combatido.

Porém, as bancas terão, agora, de levar a sério as advertências dos órgãos de segurança, porque eles

“recrutaram”, de certa forma, os grandes clientes corporativos para sua equipe de pressão. Alguns desses clientes já informaram as bancas que não mais confiarão a elas serviços jurídicos em que informações sensíveis estejam envolvidas se os advogados não comprovarem que dispõem de um sistema de segurança de dados à prova de *hackers*.

Algumas corporações adotaram a prática de enviar ao escritório de advocacia um questionário com 60 perguntas, em que medidas de segurança cibernética são detalhadas. Outras corporações estão enviando especialistas em segurança aos escritórios para avaliar seus sistemas de segurança. Algumas exigem que a banca adquira uma apólice de seguro que cubra, especificamente, falhas de segurança que possam ser definidas como má prática.

“Em outras palavras, as corporações estão dizendo às bancas que não vão ver a cor de seu dinheiro se seu sistema de segurança na Internet não garantir a melhor proteção de dados disponível no mercado”, disse ao jornal o sócio diretor-executivo da Law & Forensics, Daniel Garrie. A firma se especializa em consultoria de segurança de computação para escritórios de advocacia.

O vice-presidente da Endurance Specialty Holdings, Stuart Pattison, cuja empresa fornece seguro para cobertura de responsabilidade profissional a escritórios de advocacia, disse ao jornal que “a maior preocupação do FBI é contra ataques de *hackers* patrocinados por governos estrangeiros, que invadem os sistemas de computação dos escritórios de advocacia para descobrir o que as grandes corporações americanas estão fazendo”.

Não se espera que os órgãos de segurança não saibam o que estão dizendo. Se a preocupação é grande a ponto de pressionar as bancas a tornar a segurança na Internet uma de suas mais altas prioridades, é porque o problema realmente existe. Como espionagem é, historicamente, uma via de duas mãos, as bancas em outros países também devem se preocupar com ela, quando lidam com transações que despertam o interesse de outros países.