Sequestro de dados é preocupação a escritórios de advocacia

03/09/2016

O sequestro de dados está se tornando um problema não só para grandes empresas, mas também para escritórios de advocacia. O crime ocorre da seguinte forma: *hackers* invadem os computadores, criptografam os dados e depois os escondem. Pedem, então, um resgate para permitir o acesso novamente. A prática recebeu o nome de *ransomware,* fusão das palavras inglesas *ransom* (resgate) e *malware* (tipo de programa que infecta computadores para coletar informações).

O valor para devolução das informações é normalmente cobrado em *bitcoin* (moeda digital usada para transações na internet), para evitar o rastreamento e varia conforme o caso. Normalmente não é muito alto, justamente para a vítima pagar sem muitos questionamentos, pensando que levar o caso à polícia dará mais trabalho do que atender às reivindicações.

Algumas bancas norte-americanas já foram alvo desses sequestros. Entre as vítimas estão o escritório da Flórida *The Brown Firm* — que pagou US$ 2,5 mil para reaver seus documentos digitais — e o californiano Ziprick and Cramer LLP, que não pagou o valor pedido por ter cópias das informações.

Na América Latina, 92% das vítimas de sequestro digital são brasileiras. "Já existem vários casos, mas nenhum na mídia", disse a advogada especializada em Direito Digital **Juliana Abrusio** durante encontro do Centro de Estudos das Sociedades de Advogados, nesta terça-feira (30/8).

Reprodução

Para Juliana Abrusio, clientes devem ser o foco da segurança digital em escritórios.
Reprodução

Juliana destacou que o foco da segurança digital em escritórios de advocacia devem ser os clientes, que são os principais motivadores indiretos desses crimes e muito afetados por uma

eventual perda de informações. Disse ainda que, segundo a *McAfee*, empresa especializada em proteção digital, as amostras de *ransomware* cresceram 169% em 2015.

O também especialista em Direito Digital **Alexandre Atheniense** citou que há, inclusive, clientes que impõem a implantação de mecanismos de segurança digital como condição para fechar contratos com advogados, bem como a adequação ao *compliance* internacional.

Ele afirmou que os profissionais do Direito costumam achar que não são potenciais alvos de ataques digitais, mas estão errados. "Se você acha que não é alvo, já está errado. Todo mundo é alvo de *hacker* em relação a vazamento de dados." Atheniense explicou que essa falta de interesse pelo tema é cultural, pois o brasileiro tem atitudes muito mais reativas do que preventivas em relação a eventuais problemas. "Deixar acontecer para saber como reagir."

O advogado reforçou que o meio digital não é totalmente seguro e que o ineditismo do tema no Brasil afeta sua compreensão. Disse ainda que o brasileiro costuma estar bem aparelhados em termos tecnológicos, mas a segurança dos dados fica em segundo plano. "Nossa cultura em lidar com o meio digital é muito recente."

Reprodução

Marcelo Fernandes ressaltou que modelo de segurança mudou, saindo do princípio de perímetro para um de várias frentes devido ao aumento da portabilidade.
Reprodução

Para **Marcelo Fernandes**, diretor de marketing da Intralinks, empresa especializada em segurança digital, o modelo de proteção mudou muito nos últimos anos, saindo de um conceito de perímetro dos computadores (o *firewall*) para um de várias frentes, que protege o documento e todos os dispositivos usados para manipulação dessas informações.

“É uma grande mudança de paradigma”, disse o executivo, ressaltando que o aumento da portabilidade com o uso intensivo de *smartphones*, *notebooks* e *tablets* aumenta a insegurança na troca de dados. “O *firewall* nem sempre é a solução mais eficiente.” Segundo Fernandes, são usados atualmente programas de segurança “embebidos” no documento, como uma espécie de vacina, que garante o acesso apenas a pessoas pré-autorizadas.

Fator humano
Apesar das preocupações dos palestrantes estarem focadas no meio digital, os três ressaltaram que o fator humano ainda é o principal causador de problemas nas trocas de informações. Trabalhadores desatentos ou mal intencionados podem prejudicar negócios ou expor clientes inesperadamente.

Jeferson Heroico

Atheniense explicou que falta de interesse pelo tema é cultural, pois o brasileiro tem atitudes muito mais reativas do que preventivas
Jeferson Heroico

Alexandre Atheniense contou que passou por esses problemas e que chegou a ser obrigado a instalar programas de monitoramento na máquina de alguns usuários que usavam o tempo de serviço para outras atividades. Ele ressaltou, porém, que o tráfego de informações por meio digital o ajudou a encontrar o problema e resolvê-lo. "Tudo que você consegue circular em meio digital aumenta a rastreabilidade de coisas que muitas vezes o papel não revelaria."

Esse aumento de controle no trânsito do documento também foi citado por Fernandes, que o chamou de *metadata tapping*, que garante o rastreamento da informação e reforça a segurança ao mesmo tempo. “A *cybersegurança* deve ser vista um risco ao negócio”, reforçou.

Juliana Abrusio também citou um caso em que um advogado de um escritório canadense especializado em crimes do colarinho branco foi a um bar depois do trabalho e, por ter esquecido seu *tablet* quando deixou o local, muitas informações dos clientes da banca estavam na internet no dia seguinte.

A advogada contou ainda outro episódio em que o chefe do departamento de tecnologia da informação de uma empresa ficou oito anos recebendo cópias ocultas de e-mails enviados entre os sócios da companhia por oito anos sem o conhecimento de ninguém.

Citando o caso canadense, Juliana ressaltou a importância de as bancas fornecerem aparelhos móveis aos funcionários para que eles atuem remotamente. Segundo ela, esse é o modelo ideal, pois a empresa pode instalar programas nos aparelhos que permitam sua inutilização imediata ou rastreamento, mas ponderou que essa estratégia deve ser bem planejada.

Conscientização necessária
A advogada afirmou que um dos principais caminhos usados por instituições para promover a segurança digital é a conscientização. Ressaltou que Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (Anbima) e o Superior Tribunal de Justiça lançaram cartilhas nesse sentido. Disse ainda que um dos melhores materiais sobre o tema foi produzido pelo Kaspersky Lab. "A contaminação pode vir em um e-mail, e, por isso, todos do escritório devem saber sobre o assunto."

Apesar da importância da conscientização, Alexandre Atheniense ponderou que as decisões sobre o tema devem vir de cima, da direção das bancas, e que o plano de contingenciamento para panes digitais precisa ser pré-definido, estabelecendo se haverá ou não uma pessoa exclusivamente responsável sobre isso, se ela será terceirizada.

Ele ressaltou ainda que o mercado de segurança e tecnologia de informação, atualmente, é bem mais barato e acessível do que há alguns anos. Segundo o advogado, o setor "virou *commodity*" e já é possível alugar a infraestrutura, tornando desnecessário pagar por licenças de software, que encareciam muito a atividade.

Juliana Abrusio também explicou que as pessoas responsáveis pela tecnologia da informação trabalham com a infraestrutura de armazenamento e de transmissão, deslocando a responsabilidade pela gestão de segurança para outro profissional, de preferência o gestor do negócio. "O advogado não precisa se cobrar tanto sobre tecnologia, ele precisa saber dos riscos para encaminhar o que precisa ser feito".

Clique aqui para acessar o material apresentado por Alexandre Atheniense no evento.

Fonte: https://conjur.jumps.com.br/2016-set-03/sequestro-dados-e-preocupacao-escritorios-advocacia/