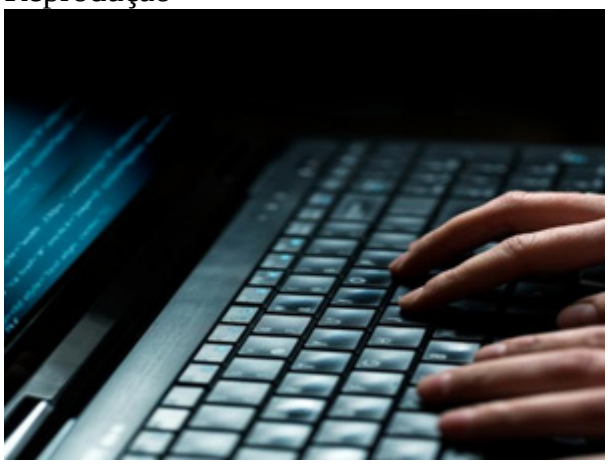
# Lei brasileira dá poucas garantias contra ataques virtuais globais

O ataque de hackers que afetou mais de 70 países acende novamente um alerta que já é conhecido no mundo da advocacia: o sequestro de dados (ou *ransomware*, no jargão da informática). Além da adoção de medidas de segurança, no âmbito da legislação disponível no Brasil, há pouco a ser feito.

"Embora a internet não tenha fronteiras, temos os limites de jurisdição e competência, então fica muito difícil responsabilizar um agente danoso que esteja situado no exterior", diz o advogado **Omar Kaminski**, especialista em Direito Digital.

Reprodução



Criminosos virtuais cobram resgate para liberar acesso a dados
Reprodução

Ele afirma que o ideal seria o Brasil ter uma legislação mais uniforme, via tratados e convenções internacionais. Para ele, o mais próximo disso é a Convenção de Cibercrimes de Budapeste, de 2001, da qual o Brasil não é signatário.

"Nossa legislação local não é a mais adequada para punir ataques cibernéticos, temos basicamente o artigo 266 do Código Penal modificado pela Lei 12.737, apelidada de Lei Carolina Dieckmann, cuja pena é aquém da desejável, e a Lei Antiterrorismo, 13.260, que prevê penas muito mais severas", analisa Kaminski.

O especialista em tecnologia **Marcelo Stopanovski** alerta que os escritórios não estão preparados para este tipo de ataque. Ele lembra que o vazamento que ficou conhecido como *Panama Papers* começou com a invasão do sistema de um escritório de advocacia e que as bancas são cada vez mais alvos visados.


2023 - www.conjur.com.br - Todos os direitos reservados.

“Proteger seu banco de dados em um servidor fora do escritório e com forte aparato de segurança digital é um primeiro ponto. Porém, vai além: o advogado tem que entender que seu notebook, seu smartphone, suas ligações e mensagens, tudo faz parte dos ativos da empresa e deve passar por processos de segurança”, explica Stopanovski à **ConJur**.

Professor da faculdade de direito do IDP São Paulo e um dos coordenadores do grupo de estudos Inteligência Artificial a Serviço da Investigação, **Alexandre Zavaglia Coelho** acompanha de perto o tema e diz que ele não é novidade.

"Essa prática tem aumentado no Brasil, e já utilizam como pedido de resgate *bitcoins*. Isso reforça a importância com a segurança dos dados das empresas e, especialmente, de seus clientes, além de uma estrutura correta de *backup*, que em boa parte desses casos pode impedir o resultado pretendido pelos criminosos”, ressalta Coelho.

Especialista em proteção de dados pela *London School of Economics*, **Thiago Luís Sombra** alerta que o episódio evidenciou a falta de um plano de contingência sobre como reagir a ataques em massa por parte de setores de tecnologia de órgãos e empresas. "Basta observar que a única sugestão apresentada em vários locais foi a retirada do equipamento da tomada".

Ele ainda explica que não há no Brasil nenhuma obrigação de se notificar as autoridades responsáveis e as pessoas cujo dados foram violados por um ataque de hackers a respeito do fato. Porém, diz, se a empresa que teve os dados comprometidos for estrangeira, ela poderá ter consequências no seu país de origem em virtude da existência de normas a respeito União Europeia e EUA.

"Se um escritório brasileiro for invadido e dados dos clientes forem vazados, o escritório poderá ser responsabilizado com base em c*ulpa em vigilando* e *culpa in custodiendo*, desde que provado o dano, a culpa e o nexo causal, se não foram adotados cuidados mínimos de segurança. Há ainda possibilidade de responsabilidade objetiva nas relações de consumo e em face do Estado", explica Sombra..

No ataque desta sexta, os computadores tinham seus dados criptografados e ele só ficariam acessíveis novamente mediante pagamento em *bitcoins* (uma espécie de moeda virtual). O ataque se aproveitava de uma brecha de segurança em versões desatualizadas do Windows.

A Microsoft afirmou ter disponibilizado, em março, uma atualização que eliminava a vulnerabilidade. Especialistas recomendam que o pagamento não seja feito, pois, por se tratar de criminosos, não há garantia de que os dados sejam recuperados. Além disso, as empresas de segurança (como os fabricantes de antivírus) trabalham em uma solução.

**Serviços**
A preocupação com este tipo de ameaça já vem de algum tempo. A última edição da Fenalaw, em São Paulo, confirmou a tendência de crescimento dos serviços de proteção das informações dos escritórios, com dados na “nuvem” e em servidores protegidos.

As empresas que atuam na proteção de dados dos escritórios  mostraram estratégias diferentes para


2023 - www.conjur.com.br - Todos os direitos reservados.

abordar a questão. A Totvs prefere manter tudo sob seu comando: “Temos nosso próprio data center não temos terceiros envolvidos”, disse **Marcelo Cosentino**, vice-presidente dos segmentos de serviços da empresa.

Já para a Hórus, o caminho é buscar parceria e criar a opção de um backup, já que em geral o dado não é subtraído, mas bloqueado. “Todo nosso ambiente é replicado em outro *data center* além do original. Os hackers tentam extorquir impedindo o acesso à informação, mas nós temos ela replicada”, contou **Fabio Cabral**, sócio da empresa.

**Ataque massivo**
Sites de pelo menos dez tribunais brasileiros deixaram de funcionar nesta sexta-feira (12/5), quando um ataque cibernético atingiu computadores de mais de 70 países. Somente o Tribunal de Justiça de São Paulo confirmou ter detectado “máquinas infectadas” e suspendeu prazos processuais. Os demais anunciaram que tomaram a medida apenas por precaução.

Nas cortes superiores, apenas o Superior Tribunal de Justiça afirmou ter tomado alguma providência. O site funcionou normalmente, mas o setor de tecnologia da informação tentou reforçar a segurança do sistema. Em São Paulo, o Ministério Público também afirmou ter deixado o site fora do ar por precaução.

Outros órgãos públicos também desligaram seus, como o Itamaraty, ministério do Trabalho e do Desenvolvimento Social e Agrário. O Instituto Nacional do Seguro Social (INSS) interrompeu o atendimento após registrar indícios de ataque. A Petrobras reiniciou a rede corporativa por causa do problema.

**Texto atualizado às 17h25 do dia 15/5/2017 para acréscimo de informações.*

**Date Created**
13/05/2017


2023 - www.conjur.com.br - Todos os direitos reservados.