A ameaça que o *Ransomware* apresenta para empresas e economia

Autores:

Leonardo Palhares
lpalhares@almeidalaw.com.br

Caio Faria Lima
cilima@almeidalaw.com.br

Abstrato:

É fundamental que as empresas comecem a tomar uma série de precauções e busquem assessoria jurídica para se resguardar contra o *Ransomware*, *malware* conhecido como "sequestrador de sistemas", devido ao crescimento no número de vítimas dessa ameaça global que impede ou restringe o acesso do usuário ao seu próprio sistema.

Um recente estudo analisa quais serão os crimes cibernéticos que irão afetar empresas e consumidores no ano de 2016. Entre elas está o *Ransomware*. Esta prática consiste na instalação de um tipo de *malware* que, quando dentro de um sistema, impede ou restringe o acesso do usuário e, na sequência, aquele em controle do sistema exige o pagamento de uma recompensa para que o acesso seja supostamente reestabelecido. É o equivalente ao sequestro do sistema por criminosos, que só o liberam mediante o pagamento de um resgate.

Essa é uma grande ameaça para empresas do mundo e poder público, visto que um ataque dessa magnitude pode inviabilizar e engessar a atividade empresarial, assim como causar a perda definitiva de arquivos.

Assim, organizamos uma lista de orientações para garantir a prevenção deste tipo de ataque:

- **Backup:** Uma das diretrizes mais importantes apontadas por especialistas em segurança cibernética consiste na manutenção de backup de todo o sistema. Com um backup completo e atualizado, caso seu sistema seja vítima deste *malware*, basta restaurá-lo e transferir os arquivos salvos.

- **Orientar funcionários:** Em uma empresa, a ação de um funcionário desinformado pode causar sérias consequências para o sistema, por isso é fundamental uma orientação para que eles não abram e-mails suspeitos, não entrem em sites duvidosos, entre outras medidas simples, mas que são essenciais para o bom funcionamento de qualquer sistema de segurança.

- **Manter o antivírus e os programas atualizados:** Uma das maneiras utilizadas pelos criminosos para entrar em um sistema é se aproveitando de falhas do mesmo como a falta de um bom antivírus e vulnerabilidades de programas e aplicativos desatualizados.

Se sua empresa detectar qualquer sinal de invasão de um *Ransomware*, é aconselhável seguir os passos abaixo:

1) Desligue o sistema: Ao desligar o sistema e a internet, você impede a transferência de seus dados pessoais para os criminosos;

2) Procurar assistência jurídica: Uma vez identificado o ataque, é fundamental obter aconselhamento profissional de um advogado

especializado para que seus direitos sejam resguardados e que sejam iniciadas as primeiras providências, como o contato com autoridades locais para que estas fiquem cientes da quantidade de ataques realizados e do *modus operandi* dos criminosos, possibilitando a condução de uma investigação eficiente.

O pagamento do resgate **NÃO** é aconselhável porque além de ajudar a financiar essa atividade, muitas vezes os criminosos não liberam o sistema.

Uma vez seguidas estas diretrizes preventivas, caso a empresa, ainda assim, seja alvo de ataque *Ransomware*, é possível também buscar reparação diretamente no Judiciário. É possível provocar, inclusive, uma aprofundada investigação policial com o objetivo de determinar a origem dos ataques e, então, requerer reparação civil pelos danos causados, bem como a condenação criminal dos envolvidos.

O Almeida Advogados possui uma equipe especializada em Tecnologia que está sempre atenta às novidades no Brasil. A equipe está à disposição para esclarecer quaisquer dúvidas sobre essa ameaça e auxiliar as empresas que forem vítimas desse ataque.