

Ransomware: um alerta para as empresas terem políticas confiáveis de segurança

Vice-presidente de Cloud e Segurança da Juniper Networks alerta sobre o novo ataque e indica alguns caminhos para as corporações se protegerem.

01/09/2016 15:35:58

A atividade de todo tipo de empresa, tanto em sua administração interna quanto na relação com clientes e fornecedores, depende hoje quase completamente de sistemas e aplicações em redes conectadas à Internet. Nesse cenário, questões referentes à segurança da rede não são mais um problema isolado do setor de tecnologia da informação – são críticos para os negócios.

O ransomware, ataque no qual criminosos entram nos sistemas corporativos por meio da rede, criptografam todos os dados da empresa e exigem um resgate para liberá-los.

Um caso recente é o do hospital Hollywood Presbyterian Medical Center, de Los Angeles, que foi uma das vítimas de ransomware e teve que pagar US\$ 17 mil para liberar sistemas tomados reféns por criminosos. Durante o ataque, a equipe do hospital teve que voltar a fazer registros dos pacientes em papel e enviar muitos doentes de alto risco para outros hospitais. Quando o dia a dia de uma organização depende tanto de computadores e acesso à internet, ficar sem acesso a seus sistemas pode ser uma catástrofe.

O ransomware é um tipo de ataque específico, mas, de uma forma mais geral, ele serve de alerta para as empresas sobre a necessidade de ter uma política de segurança e sobre os danos que os ataques podem causar não apenas em termos financeiros, com o pagamento de resgates e a perda de transações, mas à reputação das empresas. E a estratégia que ela sugere para avaliar a possibilidade de pagamento de resgates é também uma amostra de como questões relativas à segurança devem ser discutidas e planejadas.

Ao criar uma estratégia e considerar se deve ou não pagar resgates as empresas devem considerar os seguintes itens:

1. Back-up e Imaging dos Dados – Com o crescimento exponencial de dados corporativos, é difícil para as empresas definir quais informações devem ser armazenadas. Este conhecimento, no entanto, é crítico no momento de decidir pagar ou não um resgate. Se uma empresa tem um backup consistente dos dados sequestrados, pode reverter a situação com a restauração do backup sem

precisar dar dinheiro a criminosos.

2. Importância dos Dados – As empresas devem fazer um inventário de seus dados e sistemas, identificar as peças críticas para sua operação e então decidir quanto podem gastar para recuperar determinado dado em caso de ataque. Definir critérios específicos com antecedência torna mais fácil responder a uma exigência de resgate em caso de ataque.

3. Danos à Reputação – Ter seus dados sequestrados por criminosos nunca é bom, mas pode ser particularmente ruim para organizações que se dedicam a proteger e servir comunidades, como agências de defesa da lei e hospitais. Além da importância dos dados comprometidos, as organizações devem considerar como a reação a um ataque de ransomware pode afetar sua reputação junto a clientes, parceiros e acionistas.

4. Considere a responsabilidade – Pagar o resgate pode ser a maneira mais fácil de liberar seus dados, mas nunca haverá uma garantia de que os criminosos vão liberar suas informações – afinal, trata-se de ladrões profissionais. De acordo com o FBI, a maioria das empresas que paga os resgates recebe seus dados de volta. Mas outro argumento é o de que pagar encoraja os criminosos e os ajuda a aperfeiçoar seus ataques.

*Jennifer Blatnik é vice-presidente de Cloud, Segurança e Marketing Corporativo da Juniper Networks.