Por Ana Albuquerque*

Recentemente, o mundo testemunhou um avassalador ataque hacker que, praticamente, levou o sistema de saúde da Romenia ao colapso. Em fevereiro, um grupo de cibercriminosos – que não foi identificado – realizou uma série de ataques a mais de uma centena de instituições de saúde romena.

O ciberataque, utilizando sequestro de dados, conhecido como malwares, paralisou serviços essenciais, causou transtornos nos atendimentos de emergência e refletiu em diversos procedimentos médicos de forma geral. Até mesmo hospitais infantis foram atingidos.

Os hackers pediram como resgate 3,5 bitcoins (cerca de R$ 890 mil), que não chegaram a ser pagos. Mas, durante quase 48 horas, todo sistema de informação médica do País ficou comprometido, refletindo no atendimento da população.

No Brasil, tivemos um caso semelhante no final de janeiro. O Instituto Nacional de Câncer (Inca), no Rio de Janeiro, também foi alvo de um ciberataque, que prejudicou todo o sistema tecnológico do local, refletindo no atendimento da população, que teve consultas adiadas e procedimentos médicos comprometidos, como a radioterapia.

Independente da região do mundo, esses ataques acendem um alerta muito importante: a vulnerabilidade dos órgãos públicos frente aos ataques hackers.

Ao contrário das empresas privadas, que investem milhões de dólares em segurança digital, os órgãos públicos nem sempre possuem condições de aprimorar sua segurança digital. Falta, muitas vezes, verbas para implementar efetivos sistemas de mitigação de risco e de proteção.

Contudo, é importante destacar que já demos um passo significativo nesse sentido. Em dezembro do ano passado, o governo federal assinou o decreto que institui a Política Nacional de Cibersegurança, tornando a segurança digital uma política governamental.

O principal ponto desse decreto é que ele trata da resiliência cibernética como um todo, trazendo respostas que os órgãos podem dar quando se tem um incidente digital, e valorizando à cultura de cyber proteção, onde será possível conscientizar as pessoas e as instituições de todo Brasil.

Por meio de treinamentos e testes, adoção de procedimentos, implementação de controles e um efetivo plano de resposta, podemos reduzir consideravelmente os efeitos destrutivos dos ciberataques. No entanto, o processo de implementação das políticas definidas por este decreto, que envolvem um comitê com diversos representantes, por exemplo, ainda está na esfera federal.

Ainda existe um longo caminho para que essas políticas internas cheguem na ponta da linha, como municípios e órgãos públicos menores. A Lei Geral de Proteção de Dados (LGPD) trouxe profundas e relevantes melhorias à segurança da informação, que foi um passo muito importante e que trouxe a relevância do tema para discussão em todas as empresas, mas ainda há muito o que se fazer e proteger.

Basta uma rápida pesquisa no Google para vermos dezenas de relatos que confirmam a vulnerabilidade do ambiente das empresas e afetam o dia a dia de todos. Neste ano, juntamente com o INCA, também há relatos de ciberataques contra Órgãos Governamentais, que têm sido frequentemente alvos de ataques cibernéticos, como a Câmara Municipal de Curitiba e o Tribunal de Justiça do Paraná, o que reforça o impacto desses ataques para toda a população.

As ameaças cibernéticas estão cada vez mais próximas e presentes, sendo importante a conscientização de todas as Entidades, sejam elas públicas ou privadas, na implementação de sistemas protecionais cibernéticos, além da verificação das vulnerabilidades e dos controles

mínimos de segurança da informação.

---

*Ana Albuquerque é Head de linhas financeiras da WTW

(03.05.2024)