Empresas do setor de saúde, instituições financeiras, comunicações, mídia e tecnologia estão entre as mais vulneráveis a ataques cibernéticos e já foram vítimas de ataques de hackers nos últimos 12 meses

O crescente uso de tecnologias como inteligência artificial, a Internet das Coisas e robótica expôs mais as empresas às ameaças de ataques de hackers. Os prejuízos no mundo com ataques cibernéticos já geram perdas de US$ 1 trilhão para as empresas, bem acima dos US$ 300 bilhões de perdas com desastres naturais em 2017, segundo relatório **Cyber Handbook 2019** da Marsh & McLennan Companies.

Segundo Javier Duran, Diretor de Risk Management da consultoria de risco e corretora de seguros Marsh Brasil, embora as novas tecnologias tenham potencial para melhorar a produtividade e a eficiência de uma empresa, elas não são implantadas considerando o grau em que elas podem aumentar a exposição cibernética da empresa. "É preciso mudar a mentalidade de como seria a gestão de risco cibernético, as organizações devem internalizar que não é uma questão de "se", mas "quando" elas irão sofrer um ataque. Isso vai reequilibrar a forma como as empresas investem e alocam seus recursos de gerenciamento de risco cibernético", afirma.

Empresas de saúde, instituições financeiras e telecomunicações são as maiores vítimas de hackers

As empresas do setor de saúde são as mais vulneráveis a ataques cibernéticos e 27% relatam já terem sido vítimas de ataques de hackers nos últimos 12 meses. Em segundo lugar estão as instituições financeiras (20%), e em terceiro as empresas de comunicações, mídia e setor de tecnologia (14%). "Os principais riscos para as empresas da área de saúde hoje incluem a exposição dos dados do paciente, exposição compartilhada de dados do sistema e exposição dos funcionários. Em 2017, o ataque global WannaCry teve sucesso em temporariamente desligar os sistemas de TI de hospitais em todo o mundo, diz o executivo.

Javier explica que entre os maiores impactos das perdas com ataque cibernético estão a interrupção dos negócios, danos na reputação corporativa e violação de informações dos clientes. Segundo o estudo, o risco de primeira parte, que não envolve roubo de informações de terceiros, passou a ser visto como principal risco cibernético. Outro ponto que ganhou visibilidade nos comitês executivos é a Lei Geral de Proteção de Dados, que entra em vigor no país em 2020. "Á medida que as organizações se tornam cada vez mais dependentes de tecnologia, o problema passa a ser a vulnerabilidade presente dentro de sua própria infraestrutura digital, que pode resultar em interrupção comercial significativa ou danos à propriedade", diz.

Para as instituições financeiras, segundo ele, as ameaças cibernéticas estão em permanente evolução em complexidade e intensidade, mas as tecnologias emergentes, como a permissão de blockchains, podem contribuir para a redução do risco e proteger adequadamente os interesses financeiros dos consumidores. "As empresas devem implementar sistemas que possam barrar a propagação de um ataque cibernético de contágio e que permitam retomar as operações da forma mais rápida possível", explica.

Contratação de seguros

Segundo o relatório, estimulado pela onda de ataques e pelas novas regras de proteção de dados, o prêmio anual de seguros cibernéticos cresceu 34% ao ano nos últimos sete anos. "As apólices de seguro cibernético são projetadas para cobrir tanto a perda direta quanto a responsabilidade por um evento cibernético", explica o Diretor da Marsh.

Fonte: ConteudoNet, em 13.05.2019.