Por Ana Albuquerque*

O Brasil assumiu uma posição de destaque quando o assunto é segurança digital. Atualmente, somos o principal alvo de ataques hackers na América Latina e estamos entre os cinco principais alvos do mundo.

O principal objetivo dos criminosos são danificar ou destruir as redes de sistemas, assim como acessar dados sigilosos, podendo causar roubo de identidade e extorsão. As empresas poderão ter seus serviços paralisados, causando perdas financeiras significativas, podendo comprometer toda a cadeia de produção e atividade da empresa. Não existe uma regra, mas, normalmente, setores de telecomunicações, instituições financeiras, educação, saúde, logística, varejo e governos são os mais visados.

Por causa disso, muitas empresas estão recorrendo ao seguro de Cyber, como uma forma de mitigar os impactos de perdas financeiras em caso de ataques cibernéticos, que causam violações de dados ou paralisação, parcial ou total, de suas atividades. De acordo com dados da Superintendência de Seguros Privados (Susep), essa modalidade de seguros registrou um crescimento de mais de 22% comparado com os 5 primeiros meses em 2023 com o mesmo período do ano anterior.

Isso porque as formas como os ataques hackers estão acontecendo varia muito, indo desde ofensivas DDoS, que consistem em bombardear servidores com solicitações até que os serviços fiquem lentos ou caiam, até os ransomware, modalidade de ciberataque que sequestra os dados e informações, só devolvendo-os mediante resgate.

Para se ter uma ideia do potencial desses ataques, em abril deste ano, a Eurocontrol, organização europeia de controle de tráfego aéreo, foi alvo de ataques DDoS do grupo russo KillNet, que tinha como objetivo interromper o tráfego aéreo na Europa. Apesar da tentativa, os voos não foram interrompidos.

Já um levantamento divulgado pela empresa de software de segurança Immunefi, trouxe os dez principais ataques com ransomware no mundo desde 2020. Somados, eles geraram um prejuízo de US 69,3 milhões. Segundo levantamento da Alto Networks, em um ano, o Brasil registrou incremento em 51% de ataques de ransomware.-.

E a tendência é que esses ataques sejam cada vez maiores e mais frequentes.

De acordo com dados da empresa de cibersegurança Netscout, o Brasil é o maior alvo de ataques DDoS da América Latina, respondendo por quase 40% de todas as ações criminosas realizadas no segundo semestre de 2022. Isso representa um aumento de 19% no número de ataques na região, se comparado com o mesmo período de 2021.

Quando falamos do sequestro de dados, os números também são alarmantes. Segundo o relatório anual The State of Ransomware da Sophos, empresa global especializada em cibersegurança, quase 70% das empresas brasileiras ouvidas sofreram ataques de ransomware no ano passado. Esse número é 13% maior do que o registrado em 2021.

Para contratar o seguro de Cyber, as empresas também precisam fazer a parte delas, implementando controles mínimos de segurança que são exigidos pelo mercado, como a implementação da autenticação multifator (MFA) para todos os seus dispositivos, empregar solução de detecção e resposta de endpoint, possuir backups separados de sua rede principal, possuir política de criptografia de dados, fazer treinamentos sobre phishing e outras técnicas de engenharia social e possuir um Plano de Continuidade de Negócios e/ou Plano de Recuperação de Desastres. Vale lembrar que as empresas podem sofrer perdas significativas com extorsão, recuperação de dados, interrupção de sua rede, responsabilidade civil por violação de dados, além

de multas e penalidades cíveis e administrativas impostas pela Autoridade Nacional de Proteção de Dados em processo administrativo.

O setor de seguros tem muito a agregar na segurança digital das empresas, temos um papel estratégico, auxiliando e orientando, mas cabe às companhias também se preparem a essa nova realidade, adotando as melhores práticas existentes no mercado.

*__Ana Albuquerque__
é Head de linhas financeiras da WTW

(12.09.2023)