Depois de quase três anos de uma mudança no modelo de trabalho, a inevitável transformação digital e inúmeros ataques de ransomware, a maioria dos líderes empresariais já não confia em sua capacidade de gerenciar o risco cibernético, em comparação com dois anos atrás. Esta é a conclusão de um novo estudo produzido pela Marsh, líder mundial em consultoria de riscos e corretagem de seguros, em parceria com a Microsoft.

Intitulado **Relatório do Estado da Resiliência Cibernética**, o levantamento foi feito com 660 tomadores de decisão sobre riscos cibernéticos no mundo, 162 deles na América Latina, para analisar como o risco cibernético é visto por diversas organizações líderes em seus segmentos, inclusive em segurança digital, TI, gestão de riscos e seguros, finanças e liderança executiva. De acordo com o relatório, a confiança desses líderes nos recursos de gerenciamento de riscos cibernéticos, incluindo a capacidade de entender e avaliar ameaças cibernéticas, mitigar e prevenir ataques cibernéticos e gerenciar e responder a ataques cibernéticos, permaneceu praticamente inalterada desde 2019.

Em 2019, 22% dos entrevistados na América Latina disseram estar muito confiantes em sua capacidade de entender e avaliar ameaças cibernéticas e 18% em suas habilidades de gerenciar e responder a incidentes cibernéticos; enquanto em 2022 os valores variaram ligeiramente, com 19% e 16%, respectivamente. No entanto, ainda em 2019, 20% tinham muita confiança em suas capacidades de mitigação ou prevenção de ataques cibernéticos, enquanto em 2022 o número caiu para 12%.

"Dada a contínua ascensão do ransomware e o crescente cenário de ameaças de hoje, não é surpresa que muitas organizações não se sintam mais confiantes em sua capacidade de responder a riscos cibernéticos agora do que em 2019", observa Edson Villar, líder de Consultoria em Cyber Risk da Marsh para a América Latina.

Além disso, muitas organizações ainda lutam para entender, como parte de suas estratégias de cibersegurança, os riscos colocados por seus fornecedores e cadeias de suprimentos digitais. Apenas 43% dos entrevistados afirmaram ter avaliado o risco dos seus fornecedores ou cadeias de suprimentos.

O estudo aponta também outras constatações:

- Apenas 41% das organizações olham além da segurança cibernética e do seguro para incluir suas funções legais, de planejamento corporativo, financeiro, operações ou gerenciamento da cadeia de suprimentos na elaboração de planos de risco cibernético;

- Quatro em cada dez entrevistados na região (41%) disseram que sua organização utiliza métodos quantitativos para medir sua exposição ao risco cibernético, o que é um passo fundamental para entender como ataques cibernéticos e outros eventos podem gerar volatilidade. Trata-se de uma melhora em relação à pesquisa de 2019, quando apenas três em cada dez entrevistados (30%) afirmaram que sua organização utilizava métodos quantitativos. As taxas de seguro cibernético continuaram a subir, impulsionadas em grande parte pelo aumento contínuo da frequência e gravidade dos sinistros de ransomware, e muitas seguradoras tentaram apertar os termos e condições de cobertura, especialmente em relação ao conflito na Ucrânia.

- 63% das empresas da América Latina e do Caribe consideram que o Home Office os coloca em risco de um ataque cibernético, seguido pelo uso de dispositivos móveis pessoais de funcionários (59%);

- Metade das empresas (50%) menciona que não conseguem medir sua exposição ao risco cibernético devido à falta de talento dentro da organização.

"Os riscos cibernéticos são onipresentes na maioria das organizações. Combater com sucesso as

ameaças cibernéticas deve ser um objetivo em toda a empresa, destinado a construir resiliência cibernética em toda a organização, em vez de investimentos independentes em prevenção de ataques ou defesa cibernética", afirma Villar. "Uma maior comunicação entre as empresas pode ajudar as organizações a fechar as lacunas existentes atualmente, aumentar a confiança e informar melhor a tomada de decisões estratégicas de modo geral em torno de ameaças cibernéticas", acrescenta.

Nesse panorama, a Marsh e a Microsoft ressaltam que as empresas devem apostar em uma estratégia de prevenção abrangente e bem definida para o risco cibernético. "As empresas devem estruturar estratégias de cibersegurança com senso de urgência, levando em conta que um ataque cibernético é iminente, independentemente do ramo ou da indústria, incluindo não apenas iniciativas relacionadas à mitigação, mas também à transferência de risco através de seguros de risco cibernético", complementa Villar.

Fonte: Conteúdo Comunicação, em 18.07.2022