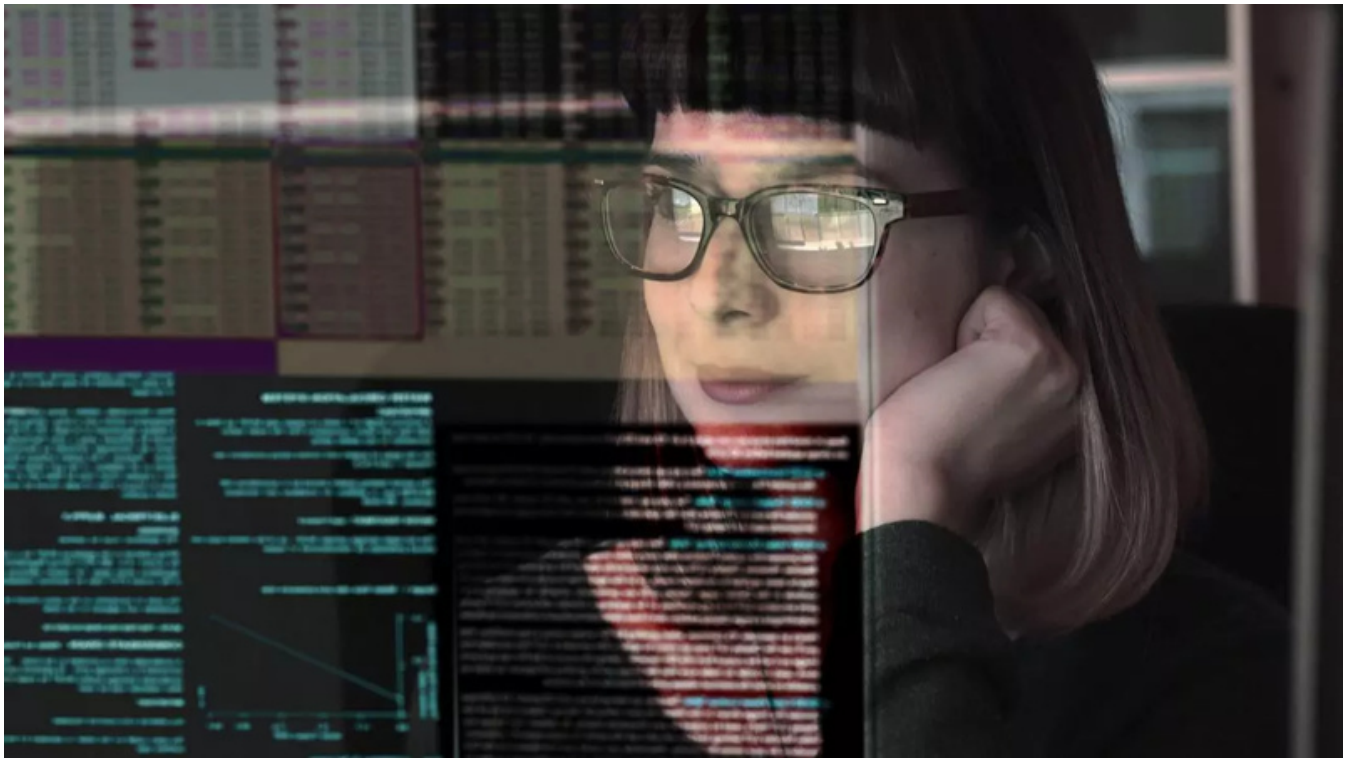

Divulgação: Aon

A Aon plc (NYSE: AON), líder global em serviços profissionais, divulgou hoje o seu **Relatório de Resiliência Cibernética 2023**, no qual apenas 15% das empresas latino-americanas consultadas indicaram ter maturidade de risco cibernético superior ao nível "básico". O relatório também mostra que as três áreas mais críticas para a região são gestão de terceiros, resiliência empresarial e segurança de aplicações, de um total de 5 aspectos qualificados.

Apesar destes números, o estudo considerou que a média de maturidade cibernética geral das empresas latino-americanas é a mesma de organizações da Europa, Oriente Médio e África, ficando atrás apenas dos índices registrados nos Estados Unidos.

O estudo foi desenvolvido para auxiliar os líderes empresariais na comparação da maturidade do risco cibernético de suas organizações com a de outras empresas, além de servir como um guia para melhor tomada de decisões na gestão desses riscos, organizado em seis áreas específicas: cibernética, operacional, cadeia de suprimentos, interno, reputacional e sistêmico.

O relatório é baseado em dados de clientes coletados a partir da Avaliação do Quociente Cibernético (CyQu) da Aon e de questionários suplementares de Ransomware e de Tecnologia Operacional. O CyQu é uma plataforma global de avaliação de risco que apoia organizações a gerenciar o risco cibernético e fornece visibilidade sobre exposições e fatores de segurança.

Em gestão de riscos de terceiros, principalmente na definição de SLAs de segurança e definição de responsabilidades, apenas 17% das empresas latino-americanas têm pontuações de risco superiores a 2,5, em uma escala que vai até 4,0. Este aspecto avalia se as companhias possuem estratégias de cibersegurança para incidentes ou ataques que possam ocorrer e envolvam terceiros, prestadores de serviço e demais partes das cadeias de suprimento e fornecimento. Os dados mostram que, em geral, as organizações da região carecem de políticas específicas de segurança cibernética para seus fornecedores, bem como necessitam de capacidades adicionais para garantir que essas políticas sejam cumpridas.

Já em resiliência empresarial, apenas 25% apresentam um perfil de risco superior ao “básico” em termos de continuidade do negócio ou em possuir um plano de recuperação de desastres focado no restabelecimento de suas operações e quantificação do impacto financeiro. Referente ao planejamento de resposta a incidentes cibernéticos e exercícios de simulação, só 35% das empresas possuem um perfil de risco superior ao “básico”. Assim, entende-se que apesar de possuírem planos de resposta ao incidente, empresas não os testam e revisam regularmente.

A pesquisa também identificou deficiências em outra importante área de controle: segurança de aplicações. Menos de 35% das empresas latino-americanas apresentaram um perfil de risco superior a “básico” nesta área, visto que não estão gerenciando adequadamente o processo de licenciamento de aplicativos de software, nem os desenvolvedores de software estão sendo treinados em questões de segurança e tampouco realizam as análises dinâmicas e testes de invasão para aplicativos. Isso pode ser resultado de uma falta de especialização das empresas em desenvolvimento, o que por sua vez faz com as empresas terceirizem essa atividade com frequência, isso nos leva de volta às falhas apresentadas no domínio de segurança sobre gestão de fornecedores.

“As empresas na América Latina e no mundo experimentaram novas formas de volatilidade nos últimos quatro anos, com o aumento na frequência e gravidade das ameaças cibernéticas e de eventos de ransomware, seguido por um mercado de seguros cibernéticos com prêmios e franquias crescentes, bem como um maior e mais rigoroso processo de subscrição", explica Sergio Torres, líder da Aon na América Latina para Serviços Financeiros & Profissionais & Cyber. “Portanto, os administradores das empresas estão mais conscientes de que os eventos cibernéticos têm potencial de impactar todas as áreas do negócio. Alcançar a resiliência cibernética é um tema recorrente para eles e a ameaça passou a ser abordada a partir de uma perspectiva holística de risco”.

Visão por setor

Considerando três setores específicos do mercado global - finanças e seguros, saúde e indústria - os dados do CyQu classificou as empresas da região com um desempenho relativamente bom em comparação aos seus pares na Europa, Oriente Médio, África e EUA, onde a posição cibernética geral atingiu o nível “gerido” em 2022.

- *Finanças e Seguros*: As empresas latino-americanas alcançaram uma pontuação média geral de 2,7 ou “gerenciado”, indicando que implementaram tecnologias e práticas de gestão de risco em toda a organização. Este nível de gestão de riscos reflete o ambiente regulatório em que estas empresas operam e um networking mais maduro. Assim, os indicadores preditivos respaldam as práticas de cibersegurança ao definirem políticas, processos e procedimentos, métodos uniformes para responder de forma eficaz às mudanças nos riscos, uma arquitetura sólida, fortes mecanismos de defesa contra violações de perímetro e cuidados vitais na segurança da rede, entre outros aspectos;

- *Saúde*: A maturidade do risco cibernético para as empresas da região parece ser a mesma dos seus pares nos Estados Unidos. No entanto, as tecnologias e práticas de gestão de riscos de cibersegurança ainda precisam ser aprimoradas, melhorando a segurança das aplicações, a resiliência empresarial, a segurança física e a gestão de terceiros. A implementação consistente de mecanismos de autenticação multifatorial nas redes é crítica, pois as violações de senha podem comprometer dados confidenciais ou possibilitar o acesso de intrusos;

- *Setor Industrial*: apresenta índices semelhantes na maioria das áreas em comparação com seus pares norte-americanos. No entanto, tal como no setor da saúde, as práticas e tecnologias de gestão de riscos de cibersegurança não são aprimoradas, têm um âmbito limitado, o risco é gerido ad hoc e, por vezes, de forma reativa. As questões mais críticas dizem respeito à gestão de terceiros, à segurança das aplicações e à resiliência empresarial.

“Conquistar resiliência cibernética e empresarial é desafiador para qualquer organização. Na Aon,

ajudamos nossos clientes a minimizar riscos financeiros, operacionais e de reputação em um ambiente volátil, trabalhando em três pontos específicos:

Primeiro, para que tenham um melhor controle na administração de terceiros, é imprescindível alinhá-los com as políticas da empresa, realizar auditorias de recuperação de desastres e preparar previsões do impacto financeiro do risco cibernético que definam as estratégias de segurança cibernética.

Segundo, a resiliência empresarial está presente quando é garantida a implementação de planos técnicos de continuidade de negócios e de recuperação de desastres. Estes planos permitirão a restauração em caso de falha crítica de software ou tecnologia, falha de um serviço público crítico ou fornecedor de tecnologia, perda ou modificação de informações vitais e divulgação de informações extremamente sensíveis, entre outros.

E terceiro, se todos os desenvolvedores concluírem um curso de treinamento em segurança com frequência, um inventário de aplicações for mantido e o software não autorizado for eliminado, a segurança das aplicações poderá ser aumentada" explica Marco Mendes, líder de Cyber e para a Aon no Brasil.

Para mais informações sobre o Relatório de Resiliência Cibernética de 2023, acesse-o na íntegra **aqui**.

Sobre a Aon

Aon plc (NYSE: AON) existe para dar melhor forma às decisões - para proteger e enriquecer a vida das pessoas em todo o mundo. Nossa equipe fornece aos nossos clientes, em mais de 120 países e territórios, consultoria e soluções que lhes dão clareza e confiança para tomar as melhores decisões para proteger e expandir seus negócios.

Siga a Aon no Twitter, LinkedIn, Facebook e Instagram. Mantenha-se atualizado acessando a Aon Newsroom e se inscreva aqui para receber alertas de notícias.

Fonte: FSB, em 01.11.2023