

A falha recente no software Falcon que resultou em um apagão global de serviços essenciais, trouxe à tona a vulnerabilidade das empresas frente aos riscos que podem causar interrupção de negócios. O incidente, que afetou aeroportos, bancos, hospitais e diversos setores em todo o mundo, destaca a urgência de uma abordagem integral na gestão de riscos operacionais e cibernéticos.

**A 9ª Pesquisa Global de Gestão de Riscos da Aon revela que a interrupção de negócios é uma das maiores preocupações para as empresas brasileiras**, posicionando-se como o risco mais crítico no país. Das empresas brasileiras entrevistadas, **63,1% relatam possuir planos formais de resposta a esse tipo de incidente**, e **69% diz ter planos formais de resposta contra ataques cibernéticos e violação de dados**.

A falha da CrowdStrike ilustra como uma interrupção operacional pode ter um impacto devastador em diversos setores em escala global. É essencial realizar avaliações abrangentes dos riscos, investir em tecnologias de segurança avançadas e promover programas contínuos de treinamento e conscientização para funcionários.

A pesquisa da Aon também destaca que apenas **22,2% das empresas brasileiras possuem planos de continuidade específicos para interrupções de negócios** e **23,2% contra ataques cibernéticos e violação de dados**, evidenciando a necessidade de maior preparação. A implementação de Centros de Operações de Segurança (SOC) pode ser um diferencial na detecção precoce de anomalias e resposta rápida a incidentes, minimizando o tempo de inatividade e os impactos operacionais.

Diante do recente incidente com a CrowdStrike, a Aon reforça a importância da governança eficaz de cibersegurança e da gestão de riscos operacionais para fortalecer a resiliência das empresas.

**Fonte:** Aon/FSB, em 19.07.2024.