Deloitte Cyber

Desafios comuns de segurança tornam organizações mais vulneráveis a ataques cibernéticos

Falta de segmentação de rede de Tecnologia Operacional (TO) e Tecnologia da Informação (TI) para impedir que ataques se expandam para redes críticas e sistemas de controles

Falta de backups de redundância que tenham sido testados para garantir a resiliência e recuperação efetiva do negócio

Gestão de vulnerabilidade inadequada e processo de hardening* ineficiente ou não abrangente

Visão limitada de coordenação de TO e TI, levando à criação de cenários isolados e segregados para desenvolvimento de respostas a ameaças de cyber e planos de resiliência

Conhecimento limitado de vulnerabilidades na área de ataque e caminhos para sistemas e ativos críticos

Falta de ferramentas modernas para prover acesso remoto e administrativo a sistemas de TO, assim como para autenticação multifator

Inexistência de plano de resposta para incidentes de ransomware para recuperar sistemas críticos e subir novamente, e falta de plano de continuidade de negócios

Disponibilidade limitada para monitorar uploads dos usuários com anomalias por meio de Análises Comportamentais de Entidade e Usuário (UEBA, na sigla em inglês) e ferramentas de Prevenção de Perda de Dados (DLP, na sigla em inglês)

*Hardening é o processo cíclico de aplicação e testes de patches