Casos recentes mostram como fornecedores mal gerenciados podem comprometer sistemas críticos de corporações – Nas grandes corporações, a crescente dependência de fornecedores, parceiros e prestadores de serviço trouxe ganhos operacionais importantes, mas também multiplicou os vetores de risco cibernético. De acordo com o Índice de Preparação para Cibersegurança 2025, da Cisco, apenas 5% das empresas no Brasil possuem maturidade suficiente para enfrentar ameaças digitais modernas, e mais de 30% já sofreram algum tipo de ataque. Com a entrada de terceiros no ecossistema digital das empresas, cresce a superfície de ataque e, com ela, a vulnerabilidade diante de incidentes de segurança.

Essa preocupação é respaldada por um caso recente: um ataque hacker ocorrido em junho contra uma empresa de tecnologia que presta serviços a bancos nacionais, atualmente sob investigação da Polícia Federal. Embora o alvo direto tenha sido um prestador de serviços, os efeitos potenciais se estenderam a instituições financeiras de grande porte, evidenciando como vulnerabilidades externas podem desencadear crises sistêmicas.

“A gestão de terceiros é um elo crítico de todo o negócio. Se não for feita com rigor, abre brechas que podem gerar impactos financeiros, operacionais e reputacionais graves”, alerta Bruno Santos, CRO da área de Gestão de Terceiros da Bernhoeft, referência nacional em consultoria empresarial.

Entre as falhas mais comuns no relacionamento com terceiros estão o uso de credenciais fracas ou compartilhadas, ausência de segmentação de rede, baixa maturidade nas políticas de segurança por parte dos fornecedores e a inexistência de monitoramento e auditoria contínuos.

Para mitigar esses riscos, é recomendada uma abordagem estruturada, combinando tecnologia, governança e cultura compartilhada de segurança. Ferramentas como Gestão de Identidade e Acesso (IAM/PAM), plataformas integradas de Governança, Risco e Compliance (GRC/TPRM), sistemas de detecção e resposta a incidentes (SIEM/SOAR), testes periódicos de vulnerabilidades e tecnologias como blockchain para rastreabilidade já fazem parte da rotina de empresas com maior maturidade digital.

Tecnologias como inteligência artificial e machine learning também ganham espaço, especialmente na detecção de comportamentos anômalos e na automatização de respostas a incidentes. “A tecnologia é essencial, mas sozinha não resolve. A gestão de terceiros precisa ser estratégica, preventiva e orientada por dados”, reforça o especialista.

Segundo Bruno, medidas como avaliação da maturidade em segurança da informação dos fornecedores, análise da superfície de ataque externa, revisão do histórico de incidentes, verificação de certificações, uso de questionários estruturados e exigência de cláusulas contratuais específicas de segurança são passos obrigatórios para mitigar riscos de forma consistente.

Além dos controles técnicos, a construção de uma cultura de segurança da informação compartilhada com os parceiros é outro pilar estratégico. Isso inclui a realização de treinamentos periódicos, auditorias in loco, fóruns de troca de informação e definição clara de expectativas de conformidade. “Não se trata apenas de impor exigências, mas de envolver os terceiros na construção de uma rede digital resiliente”, observa Fábio Josgrilberg, Head de Novos Produtos na área de Gestão de Terceiros da Bernhoeft.

Setores como financeiro, saúde, tecnologia, infraestrutura crítica e governo estão entre os que mais exigem atenção. Nestes ambientes, a sensibilidade dos dados tratados e o impacto potencial de falhas são elevados. Por isso, a integração entre as áreas de Segurança da Informação, Jurídico, Compras e Compliance é fundamental para garantir processos padronizados e respostas coordenadas a qualquer sinal de ameaça.

Conforme diretrizes do NIST CSF 2.0 e da ISO/IEC 27002:2022, práticas como o monitoramento contínuo da cadeia de suprimentos, a inclusão de terceiros nos planos de resposta a incidentes e o

controle rigoroso de segurança em contratos tornam-se essenciais para a resiliência digital das organizações.

“A gestão de riscos de terceiros exige uma abordagem contínua, estratégica e orientada por dados. Em um cenário cada vez mais regulado e interconectado, antecipar ameaças e garantir a resiliência digital passa a ser um imperativo de negócio, e não apenas uma responsabilidade da TI”, finaliza o CRO da área de Gestão de Terceiros da Bernhoeft.

(27.11.2025)