1.Third-party risk assessment

Toda organização trabalha com fornecedores de algum tipo, seja para serviços de folha de pagamento, marketing por e-mail, viagens ou aquisição de matérias-primas. Ao lidar com terceiros, parte dos dados da empresa é compartilhada, o que pode envolver informações sensíveis, como dados financeiros. Por isso, é essencial realizar uma **análise de risco** para entender como esses fornecedores protegem os dados que recebem.

Uma boa prática é incluir os requisitos de avaliação de risco nos contratos firmados com fornecedores, definindo expectativas e penalidades em caso de descumprimento. Um método comum de avaliação de risco é o **teste de penetração**, **que simula ataques a sistemas para identificar vulnerabilidades**. Esse teste pode ser um requisito interno da empresa ou uma exigência contratual com o fornecedor. Muitas vezes, empresas terceirizadas especializadas realizam esses testes, gerando relatórios sobre a segurança adotada.

Os testes de penetração seguem regras específicas, documentadas no **termo de engajamento** (rules of engagement), **que define escopo, horários, equipamentos envolvidos e contatos de emergência caso algo saia do controle**. Além disso, pode estabelecer diretrizes sobre o manuseio de informações confidenciais encontradas durante os testes.

Ao compartilhar dados com terceiros, é essencial garantir que a segurança dessas informações seja mantida. Para isso, muitas empresas realizam **auditorias regulares** para avaliar a conformidade com as políticas de segurança. Essas auditorias são geralmente previstas em contrato, sob uma cláusula conhecida como **direito de auditoria**. Normalmente, um terceiro imparcial conduz essas auditorias para garantir transparência e cumprimento das normas.

A cadeia de suprimentos também deve ser analisada sob o ponto de vista da segurança. Um exemplo de falha grave ocorreu em 2020 com a SolarWinds, cujo software foi comprometido por um ataque, resultando na disseminação de malware para milhares de clientes. Esse incidente destacou a importância da **análise da cadeia de suprimentos**, avaliando desde a obtenção da matéria-prima até a entrega do produto final.

A contratação de **avaliações independentes** pode trazer uma nova perspectiva sobre os processos internos de segurança. Empresas especializadas podem fornecer insights valiosos e ajudar na mitigação de riscos. Antes de firmar parcerias, é comum realizar um processo de **diligência prévia (due diligence), investigando informações sobre a empresa fornecedora, como histórico financeiro e reputação**.

Além disso, é importante monitorar **possíveis conflitos de interesse**. Por exemplo, um fornecedor pode trabalhar simultaneamente para um concorrente ou ter

laços familiares com executivos da empresa contratante, o que pode comprometer a imparcialidade da relação.

Uma vez que o contrato é firmado, a empresa deve continuar **monitorando o desempenho do fornecedor**. Isso pode incluir revisões financeiras, auditorias de segurança e acompanhamento de notícias e redes sociais para identificar possíveis problemas. Para isso, é útil adotar **métodos quantitativos e qualitativos de monitoramento**, como questionários para avaliar práticas de segurança e planos de recuperação de desastres dos fornecedores.

As respostas obtidas são incorporadas à **análise de risco contínua**, permitindo ajustes e melhorias na relação com os fornecedores ao longo do tempo.