Marta Helena Schuh é Diretora de Seguros Cibernéticos e Tecnológicos na Howden Brasil

O ano de 2025 já pode ser considerado um divisor de águas no que diz respeito à escalada de ataques cibernéticos. A combinação de IA, automação e redes globais interconectadas transformou o risco em algo quase inevitável. Esse novo cenário de ameaças ganhou força à medida que grupos criminosos passaram a mirar alvos de alto impacto – varejo, provedores de serviços, infraestrutura crítica, saúde e logística – ampliando não só o alcance das investidas, como também o potencial de destruição.

De acordo com dados da Check Point Research Technologies, no segundo trimestre de 2025, a média global de ataques cibernéticos por organização atingiu 1.984 ataques por semana. Na América Latina, o avanço foi acentuado: 2.803 ataques semanais, um aumento de 5% em relação ao ano anterior, com o Brasil concentrando grande parte das ocorrências.

No país, o incidente mais emblemático foi o ataque à C&M Software, intermediária do Pix, considerado o maior já registrado contra o sistema financeiro brasileiro. Cibercriminosos conseguiram comprar as credenciais de um funcionário terceirizado, obtendo acesso aos sistemas da empresa e vazando 392 GB de dados. O prejuízo estimado ultrapassou R$1 bilhão, mostrando como falhas humanas e vulnerabilidades na cadeia podem transformar um incidente em crise financeira.

O ataque à C&M Software não foi um ponto isolado. Em 2025, outras ofensivas também expuseram a dimensão global do problema. No Reino Unido, a Marks & Spencer teve seus sistemas de pagamento e logística comprometidos, resultando em paralisações, atrasos e perdas milionárias; a Salesforce, uma das maiores provedoras globais de SaaS, foi alvo de um incidente que expôs dados sensíveis e interrompeu operações de diversas pequenas e médias empresas em múltiplos países. Na Europa, hospitais sofreram ataques coordenados, evidenciando que que infraestruturas críticas permanecem vulneráveis mesmo diante de alertas contínuos.

Os ataques extrapolaram as grandes empresas e serviços digitais: o roubo do Museu do Louvre, facilitado pelo uso de senhas fracas, tornou-se um símbolo da fragilidade humana como vetor de ataque. Em um ano marcado por invasões cada vez mais sofisticadas, foi justamente uma senha banal que expôs uma das instituições mais visitadas do mundo.

No setor de transporte, ataques a prestadores de serviços de TI para companhias aéreas geraram caos em aeroportos europeus, com atrasos e cancelamentos massivos. O episódio expôs a vulnerabilidade da cadeia de mobilidade global quando um elo falha.

Esses eventos não têm em comum apenas a escala ou o nível técnico. O que os une é a exploração de fragilidades estruturais: dependência excessiva de terceiros, cadeias de fornecedores complexas, falhas de gestão, sistemas legados e controles de segurança insuficientes. Por mais robusto que seja o núcleo de uma empresa, a vulnerabilidade pode vir de fora. A cadeia digital inteira deve ser considerada, com governança de terceiros como prioridade.

Percebe-se uma clara evolução qualitativa nas táticas utilizadas: RaaS, infostealers, deepfakes e spear phishing impulsionado por IA tornaram os ataques mais dinâmicos e difíceis de detectar. Diante desse cenário, os fundamentos da cibersegurança – antivírus atualizado, firewall configurado, backups e autenticação multifatorial – continuam essenciais, mas já não bastam. A resposta estratégica exige mapeamento da cadeia, avaliação contínua de riscos, due diligence de fornecedores, auditorias e instrumentos de transferência de risco, como o seguro cibernético.

A resposta não pode mais ser reativa. É hora de as empresas brasileiras tratarem a segurança cibernética como prioridade estratégica. Para CIOs e CISOs, o momento exige ação concreta.

O ano também mostrou que prevenir não é suficiente. É indispensável estar preparado para responder não apenas com bons planos de ação, envolvendo fornecedores de TI e provedores de serviços – os quais incluem suporte jurídico e comunicação –, mas também com o preparo financeiro que o tema requer.

O risco cibernético não é uma questão mais de TI e sim uma questão estratégica de negócios. Isso se tornou um ponto de discussão no nível de conselho. As organizações que ignoraram essa prioridade enfrentaram paralisações, danos reputacionais profundos e perdas financeiras consideráveis.

O papel do seguro cibernético está evoluindo de uma rede de segurança financeira para um parceiro estratégico de gestão de riscos. As empresas mais bem-sucedidas veem o seguro não como um mero item a ser marcado na lista de requisitos, mas como um componente integral de um ecossistema de resiliência.

O legado de 2025 é simples: segurança cibernética não é custo, é competitividade. Organizações que tratam proteção como investimento e que reconhecem a responsabilidade compartilhada entre empresa e fornecedores serão as que atravessarão 2026 com mais resiliência.

(19.01.2026)