Além da indenização financeira, novas soluções oferecem monitoramento em tempo real e resposta a incidentes automatizada para combater a sofisticação dos ataques autônomos

Segundo o relatório 2025 EY Global Cybersecurity Leadership Insights, o uso de IA na simplificação e na automação dos processos de segurança cibernética gerou redução direta de custos, com economia média anual de US$ 1,7 milhão, mas uma pesquisa da Manage Engine destaca que a IA Generativa já foi utilizada em mais de 50% dos ataques recentes contra empresas brasileiras. Além disso, a Cybersecurity Ventures estimou prejuízos globais de US$ 10,5 trilhões em 2025 em ataques cibernéticos potencializados por Inteligência Artificial.

Se, por um lado, o uso de IA aumenta a rapidez e a eficácia dos seguros cyber, por outro, há a crescente sofisticação das ofensivas. “Muitos hackers utilizam agentes de IA que podem identificar vulnerabilidades e disparar malwares de forma independente, sem intervenção humana constante, por exemplo”, explica Daniel Nogueira, diretor de tecnologia da Wiz Co.

Outro grande desafio para as seguradoras e corretoras são os deepfakes, usados para aplicar golpes de fraude de identidade. O uso de voz e vídeo sintéticos para enganar executivos tornou-se extremamente difícil de detectar, desafiando as apólices que cobrem engenharia social. Além disso, as IAs proprietárias das empresas também estão em risco: invasores podem corromper os dados de treinamento da IA de uma empresa para criar falhas invisíveis de segurança. “Para o seguro, ainda existe o risco não só do ataque externo, mas também do erro interno, que pode gerar decisões incorretas e prejuízos financeiros, como no caso de alucinações e vieses”, destaca Daniel Nogueira.

O que as empresas precisam considerar

O executivo destaca que a governança de IA é um critério que tem se tornado cada vez mais significativo nas apólices de seguro cyber. “Tanto seguradoras quanto clientes estão muito mais exigentes dentro de um cenário complexo, que requer mais detalhamento e atenção, tanto por parte das empresas quanto nos descritivos das apólices.”

Um ponto importante em relação às companhias é a governança empresarial voltada para o uso de IA, que precisa considerar: o monitoramento de quais ferramentas os colaboradores podem estar usando sem autorização (Shadow AI), a implementação obrigatória de Autenticação de Múltiplos Fatores (MFA) e da Gestão de Acessos Privilegiados (PAM), o acompanhamento da evolução da computação quântica e a avaliação de seus possíveis impactos futuros sobre a segurança dos dados e os mecanismos de criptografia e o treinamento constante das equipes. “O fator humano continua sendo o elo mais fraco da cadeia de ataques cibernéticos. Treinar os colaboradores para identificar phishing gerado por IA é vital”, diz Nogueira.

O executivo detalha os pontos que as empresas precisam levar em conta na hora de contratar ou renovar um seguro cyber em tempos de IA:

Reclassificação de engenharia social: muitas apólices antigas limitam a cobertura para fraudes de intervenção humana. Com o uso de deepfakes (voz e vídeo), as seguradoras estão criando cláusulas específicas. A empresa precisa verificar se a apólice cobre fraudes cometidas por agentes sintéticos ou se exige processos de verificação humana em duas etapas para validar o sinistro.

Cobertura para Shadow AI e erros de modelo: se um funcionário coloca dados sensíveis em uma IA generativa pública e ocorre um vazamento, a seguradora pode alegar negligência grave. As empresas precisam considerar: A apólice cobre vazamentos originados em ferramentas de terceiros (SaaS de IA)? Existe cobertura para Erros e Omissões (E&O) caso a IA da própria empresa forneça uma orientação errada que cause prejuízo financeiro a um cliente?

Manutenção da higiene cibernética como condição: a apólice não é mais estática; muitas agora contêm cláusulas de garantia de controle. Se a empresa declarar que usa IA para monitoramento de rede e, no momento do ataque, essa ferramenta estava desligada ou

desatualizada, a seguradora pode se recusar a pagar a indenização.

Extensão para danos de reputação: a IA permite ataques de desinformação em massa. Algumas apólices mais inovadoras já começam a oferecer cobertura para gerenciamento de crise de imagem caso a marca seja alvo de uma campanha de difamação gerada por deepfakes ou bots de IA.

Inovações do Seguro Cyber

O diretor de tecnologia da Wiz Co aponta também as inovações que as apólices têm apresentado para acompanhar esse ritmo tecnológico. “As seguradoras deixaram de ser apenas ‘pagadoras de indenização’ para se tornarem parceiras tecnológicas”, afirma o executivo.

“Muitas apólices têm apresentado coberturas inovadoras, que vão desde a subscrição em tempo real, na qual as próprias seguradoras usam modelos de IA para analisar o risco das companhias de forma contínua, até a resposta automatizada a incidentes, onde a seguradora oferece ferramentas de SOAR (Security Orchestration, Automation and Response) que podem reduzir o tempo de resposta a incidentes em até 95%”, finaliza Daniel Nogueira.

Outras inovações apontadas pelo executivo da Wiz Co são a precificação dinâmica, na qual o valor do prêmio pode variar conforme a postura de segurança da empresa em tempo real, e os serviços de prevenção proativa, por meio da inclusão de varreduras de vulnerabilidades gratuitas e monitoramento de Deep Web como parte integrante do pacote do seguro.

Fonte: Wiz Co/InPress Porter Novelli, em 15.06.2026.