Essa tecnologia tem sido utilizada pelas organizações nos esforços de cibersegurança, que envolvem prevenção, detecção e resposta a incidentes de segurança

A inteligência artificial está sendo cada vez mais usada para proteger as empresas das ameaças cibernéticas. Análise da EY baseada em 69 estudos publicados entre 2015 e 2020 demonstra precisão média superior a 90% na detecção de spam, malware e invasões de rede. Essa porcentagem é um dos destaques do estudo **"2024 Global Cybersecurity Leadership Insights"**, que entrevistou líderes em cibersegurança de empresas provenientes de cinco setores econômicos e atuantes nas Américas; Ásia-Pacífico; e Europa, Oriente Médio, Índia e África. Essa capacidade da IA é decorrente principalmente da aprendizagem profunda ou deep learning que permite a essa tecnologia analisar volume maior de dados e mais heterogêneo em tempo real.

"O autotreinamento com aprendizado constante está **acelerando a automação**. A IA tem ajudado as equipes cibernéticas a monitorar continuamente as redes e aplicações, por meio da prevenção e detecção das ameaças quase em tempo real. Isso leva a uma resposta mais rápida aos incidentes de segurança caso eles ocorram", diz Demetrio Carrión, sócio-líder da EY Latam para cibersegurança. Essa utilização da inteligência artificial em cibersegurança não pode ser considerada recente. O levantamento da EY constatou aumento acentuado na investigação, nas patentes e nos investimentos cibernéticos relacionados com IA desde 2015. A IA faz parte agora de 59% das patentes cibernéticas e representa a principal tecnologia em cibersegurança desde 2017.

Há, no entanto, muitas empresas que ainda não se organizaram para contar com um esforço estruturado voltado para a cibersegurança. No Brasil, o grau de maturidade corporativa é apenas mediano, de acordo com estudo recente da Abrasca (Associação Brasileira das Companhias Abertas) em parceria com o The Security Design Lab (SDL). Em uma escala de zero a dez, as 109 companhias pesquisadas de setores como agronegócio, educação, energia, financeiro, óleo e gás, saúde e tecnologia alcançaram uma nota média de 4,9. Mais de quatro em cada dez (42%) não têm um plano de resposta a incidentes de segurança; 65% não orientam a equipe para lidar com esses tipos de incidente; e 73% não dispõem de mecanismos de controle de acesso para alguns dos seus sistemas.

Serviços integrados de cibersegurança

"A cibersegurança precisa ser vista como a **integração de diversos serviços** que farão com que a empresa esteja preparada para prevenir, detectar e responder rapidamente a um incidente", explica Daniela Ceschini, associate partner da EY em Cybersecurity, que atua no Cyber Fusion Center (CFC), uma evolução do Security Operation Center (SOC), por integrar funcionalidades essenciais como resposta a incidentes, análise forense, inteligência de ameaças cibernéticas, gerenciamento de riscos de terceiros e gestão de crises. Entre esses serviços está o Cyber Threat Intelligence, que faz a busca na deep e na dark web para identificar potenciais ameaças para as empresas e seus executivos. "A partir do momento que a empresa é citada em alguns desses fóruns, ela pode ligar o sinal de alerta como forma de intensificar os esforços em cibersegurança", diz Daniela.

Destaque também para os testes de invasão no ambiente da empresa. Chamadas de ethical hacking, essas simulações podem ser feitas por meio de phishing, aqueles e-mails ou links que, ao serem abertos, costumam levar a uma invasão do sistema. "Há o fator humano que é considerável nesses casos. Por isso, esse teste serve também para treinar os colaboradores para que eles não sejam enganados pelos cibercriminosos. Verificamos, ainda, o grau de resiliência da empresa, ou seja, se ela sabe exatamente o que precisa ser feito em um incidente de segurança para retomar rapidamente o controle dos seus sistemas e ambientes de acesso", finaliza Daniela.

ISO 27001

O Cyber Fusion Center, da EY, recebeu recentemente a certificação ISO 27001, que define os

requisitos, processos e normas a serem seguidos para garantir uma gestão de segurança da informação eficaz. “A certificação abrange toda a jornada do cliente – desde a implementação até os serviços gerenciados. Com ela, fechamos o ciclo completo de cibersegurança, oferecendo um caminho integrado e contínuo do começo ao fim”, diz Marcia Bolesina, sócia de cibersegurança da EY Brasil.

Fonte: Agência EY, em 07.06.2024.