Como a inteligência artificial impacta a cibersegurança

É incontestável: a Inteligência Artificial (IA) impacta todas as indústrias. As vantagens são inegáveis, mas os ciberataques potenciados por IA são uma das maiores preocupações e lideram mesmo as classificações de risco emergente da Gartner no segundo trimestre de 2024

Ana Rita Almeida
mailto: ralmeida@hipersuper.pt
photo: DR

Estima-se que sejam necessários 4 milhões de profissionais para preencher a crescente lacuna na força de trabalho no setor da cibersegurança. O 2024 Global Cybersecurity Skills Gap Report da Fortinet revelou que 70% das organizações indicaram que a escassez de competências em cibersegurança cria riscos adicionais para as suas organizações.

O estudo conclui que as organizações estão a atribuir cada vez mais as violações de segurança à lacuna de competências em cibersegurança, que as violações de segurança continuam a ter repercussões significativas para as empresas, e os líderes executivos são frequentemente penalizados quando estas ocorrem. Também se conclui que as certificações continuam a ser altamente valorizadas pelos empregadores como uma validação das competências e conhecimentos atuais em cibersegurança e que existem inúmeras oportunidades para contratar talento e ajudar a enfrentar a escassez de competências. A frequência crescente de ciberataques dispendiosos, combinada com o potencial de consequências pessoais severas para membros do conselho e diretores, está a resultar numa pressão urgente para fortalecer as defesas cibernéticas >>>

>>>

nas empresas. Como resultado, as organizações estão a focar-se numa abordagem tripla para a cibersegurança que combina formação, consciencialização e tecnologia: ajudar as equipas de TI e segurança a obter competências vitais de segurança, investindo em formação e certificações para alcançar este objetivo, cultivar um pessoal de linha de frente ciente de cibersegurança, que possa contribuir para uma organização mais segura como primeira linha de defesa e usar soluções de segurança eficazes para garantir uma postura de segurança robusta.

Este estudo envolveu mais de 1850 decisores de TI e cibersegurança de 29 países e localidades. Os inquiridos fazem parte de diversos setores de atividade incluindo tecnologia (21%), indústria transformadora (15%) e serviços financeiros (13%).

INTELIGÊNCIA ARTIFICIAL E CIBERSEGURANÇA

Durante o segundo trimestre deste ano, um inquérito realizado pela Gartner, Inc. destaca uma preocupação crescente com ataques maliciosos aprimorados por inteligência artificial (IA) como o principal risco emergente para as empresas. Este estudo, que envolveu 274 executivos seniores de risco empresarial, também revelou novas preocupações em relação a alvos de ransomware vulneráveis.

Três dos cinco riscos emergentes mais citados pertencem à categoria tecnológica, sendo que a nova preocupação com alvos de ransomware vulneráveis entrou no radar pela primeira vez. A crescente polarização política, que surgiu pela primeira vez no rastreador no quarto trimestre de 2023, manteve-se como a terceira preocupação mais citada, enquanto o desalinhamento do perfil de talento organizacional subiu do quinto para o quarto risco mais citado.

"FORMAÇÃO CONTÍNUA DAS EQUIPAS DE SEGURANÇA É CRUCIAL"

Paulo Pinto, securing cloud and digital transformation da Fortinet Portugal, considera que a inteligência artificial (IA) é utilizada tanto para inovar os sistemas de defesa, quanto para realizar ciberataques. "Uma atividade que está a evoluir de forma alarmante, com os cibercriminosos a adotarem cada vez mais esta tecnologia para aumentar a sofisticação e a eficácia das suas táticas e dos seus ataques" confirma em conversa com o Hipersuper.

Paulo Pinto explica qu e a IA "permite automatizar e personalizar ataques de phishing, corrigindo erros de gramática e formatação, o que os torna mais difíceis de detetar. Além disso e tal como referido, a IA pode analisar grandes volumes de dados para identificar vulnerabilidades específicas, orquestrando ataques altamente direcionados. Esta evolução contínua exige que as empresas estejam sempre um passo à frente, adotando soluções avançadas para se protegerem contra estas ameaças emergentes".

Paulo Pinto, securing cloud and digital transformation da Fortinet Portugal

Na sua opinião, para mitigar os riscos associados aos ataques potenciados por IA, as empresas devem investir em tecnologias de cibersegurança igualmente avançadas. E exemplifica: o FortiAI, integrado no Fortinet Security Fabric, que utiliza IA generativa para melhorar a deteção e resposta a ameaças em tempo real, permite identificar padrões suspeitos e automatizar respostas a incidentes, reduzindo significativamente o tempo de reação, aumentando a segurança e a privacidade dos dados. Para o responsável, a formação contínua das equipas de segurança é igualmente crucial "para garantir que os profissionais estejam preparados para enfrentar estas ameaças, combinando a inteligência artificial com a expertise humana para uma plataforma de cibersegurança cada vez mais eficaz".

João Mira Santiago, executive director da Claranet Portugal, confirma a evolução rápida da utilização de IA para realizar ataques, assim como novas formas de contra-ataque. "Algumas fórmulas eficazes de defesa passam pelo investimento em recursos especializados para reforço de competências e conhecimento, investimento em sistemas de cibersegurança de última geração, tecnicamente robustos, e pela promoção de uma cultura de melhoria contínua dentro da organização para que, desta forma, se mantenham atualizados todas as ferramentas e recursos aplicados na segurança da informação", destaca. "Salientamos ainda a importância de efetuar auditorias regulares aos processos que possam ajudar a monitorizar todas as fragilidades e manter a conformidade com as normas e regulação aplicadas ao sistema, reforçando a gestão de risco. Assegurar processos de autenticação eficientes para prevenir intrusões e examinar cuidadosamente o dossier de segurança da informação de modo a compreender como os agentes do mercado estão a aperfeiçoar as suas táticas e metodologias de invasão da privacidade – pessoal e corporativa", acrescenta.

João Mira Santiago, executive director da Claranet Portugal

David Grave, security director da empresa Claranet Portugal

David Grave, security director da empresa Claranet Portugal, reforça: "para além das medidas mencionadas, é vital estabelecer um sistema de inteligência de ameaças que utilize IA para identificar e prever novas táticas e técnicas utilizadas pelos atacantes". O responsável considera vital "a colaboração entre diferentes setores e a partilha de informações sobre ciberameaças", "essenciais para construir uma defesa mais robusta e abrangente". "Implementar tecnologias de deteção de anomalias baseadas em IA pode ajudar a identificar e neutralizar ataques antes que causem danos significativos. Em última análise, uma abordagem de segurança em camadas, que combine a inteligência artificial com medidas tradicionais de cibersegurança, criará uma defesa mais resiliente e dinâmica contra ataques cada vez mais sofisticados", destaca.

Javier Castro Bravo, diretor de cibersegurança da Stratesys, explica como é que a IA pode, nas mãos

Javier Castro Bravo, diretor de cibersegurança da Stratesysww

dos cibercriminosos, ser uma ameaça: a IA pode criar emails de phishing altamente personalizados e convincentes, enganando os colaboradores para que revelem informações sensíveis ou executem ações maliciosas, os chatbots e assistentes virtuais controlados por IA podem realizar ataques de engenharia social mais sofisticados, interagindo com os colaboradores em tempo real e recolhendo informações sensíveis através de burlas complexas e a IA pode gerar deepfakes altamente convincentes, utilizando imagens, vídeos ou áudios falsos e utilizá-los para se fazer passar por executivos ou colaboradores com cargos de chefia, facilitando a fraude financeira ou o acesso a informações críticas.

O responsável desta multinacional tecnológica não tem dúvidas: os ataques estão mais automatizados, inteligentes e autónomos. "Os cibercriminosos podem utilizar a IA para automatizar e escalar os seus ataques, permitindo a execução simultânea de múltiplos ciberataques contra diferentes alvos, aumentando a eficiência, a taxa de sucesso e o impacto. Os ataques automatizados existentes, como a força bruta, a negação de serviço, etc., serão intensificados à medida que for acrescentada uma solução adicional que pode tomar decisões com base nos resultados e no progresso do ataque" começa por referir Javier Castro Bravo.

Os atacantes podem também "desenvolver malware que se adapta e aprende com os ambientes em que entra, escapando mais eficazmente às soluções de segurança tradicionais e ajustando-se aos mecanismos de defesa específicos de uma empresa" acrescenta.

Os sistemas baseados em IA podem também "analisar padrões no comportamento das soluções de segurança de uma empresa e ajustar-se em conformidade para evitar a deteção, utilizando técnicas como a análise de padrões e a geração de tráfego malicioso que imita um comportamento legítimo".

A democratização do conhecimento sobre geração de ataques é também frisada pelo diretor de cibersegurança da Stratesys que lembra que "a utilização da IA para conceber ataques elimina a barreira à entrada que, anteriormente, exigia conhecimentos técnicos avançados por parte dos cibercriminosos".

Ben Aung, chief risk officer da Sage, também não tem dúvidas: a IA pode ser uma ferramenta para fazer o bem, mas também pode contribuir para o aparecimento de novos conteúdos maliciosos e para melhorar os métodos existentes. "Por exemplo, a IA pode agora gerar mensagens de email de phishing altamente convincentes que parecem e >

>>>

soam como um ser-humano e ultrapassam muitos problemas gramaticais e linguísticos que os criminosos enfrentaram ao produzir mensagens de phishing no passado", confirma". "Este tipo de facilidade de personalização aumenta a probabilidade de enganar os utilizadores para que revelem informações sensíveis", lamenta.

"Para mitigar esses riscos, é essencial ter uma abordagem multifacetada", avança. E há boas notícias na sua opinião: a IA também pode melhorar a cibersegurança de forma significativa. "As organizações devem promover uma forte cultura de segurança, garantindo que os funcionários estejam bem informados sobre os princípios básicos de cibersegurança e o surgimento de novas ameaças. Um planeamento e processos robustos de resposta a incidentes também fazem uma grande diferença, independentemente do tipo de ataque", afirma Ben Aung.

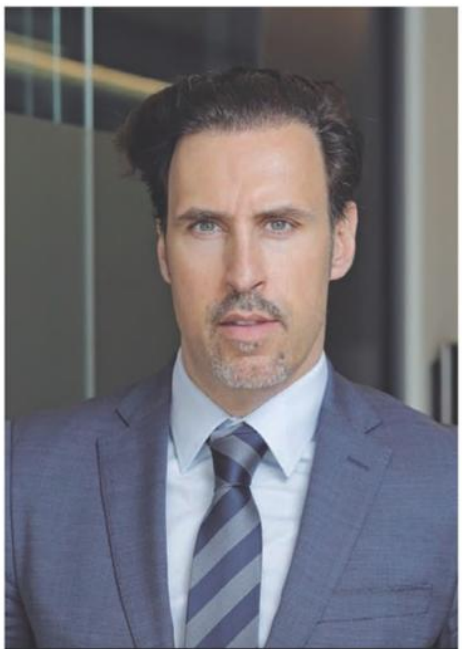
Na mesma linha, Bruno Castro, fundador e CEO da VisionWare, reconhece que os cibercriminosos estão constantemente a procurar novas formas de inovar as suas estratégias de ciberataque e a IA tem um grande potencial também de incremente inteligência e inovação nesse campo. "Os algoritmos de Machine Learning potenciam ataques direcionados com maior precisão (como spear phishing dinâmico) e também malware mais sofisticado e eficaz", considera.

Para Bruno Castro, também em termos de fraude, a integração da IA é uma preocupação, "já que, observamos cada vez mais um aprimoramento em técnicas de falsificação e usurpação de identidade e de aprendizagem de padrões de comportamento financeiro". O especialista em cibersegurança e investigação forense, confirma que "no fundo, a IA veio impulsionar as técnicas de identificação e exploração de vulnerabilidades de forma mais rápida e eficaz que os métodos tradicionais".

"Outro fator que também temos observado diz respeito à engenharia social, nomeadamente, como a IA consegue automatizar várias morfologias de ciberataques através da criação de perfis falsos e tornar a interação com os colaboradores mais autêntica e até, sofisticada", acrescenta.

No entanto, também lembra que "a cibersegurança está em constante evolução, e assim como a IA tem impactado o ataque, o mesmo acontece do lado da defesa". Para o responsável, não existe uma 'receita milagrosa' para combater estes riscos, mas sim a implementação de uma estratégia global de incremento da maturidade em cibersegurança. "Pode ser através da implementação de um SOC (Security Operations Center) que deverá incrementar a capacidade de deteção e resposta a ações maliciosas, como a implementação de sistemas evoluídos de cópias de segurança que permita estabelecer mecanismos de imutabilidade e encriptação avançada, ou ter políticas claras de governance de cibersegurança, ou ainda na prevenção de ameaças dentro da organização através de formação de colaboradores" diz. "Além disto, muitas organizações recorrem ainda, e cada vez mais, a soluções avançadas de IA para combater ciberameaças também elas impulsionadas por IA", reforça. "A IA veio para ficar e será certamente uma mais-valia também para as equipas de cibersegurança", conclui.H

Ben Aung,
chief risk officer da Sage



Bruno Castro,
fundador e CEO da VisionWare