O papel "essencial" da cibersegurança num mundo cada vez mais digitalizado

Tecnologia ■ Num contexto de desafios, a inteligência artificial assume preponderância. Arlindo Oliveira lembra que é uma tecnologia de "duplo uso". Paulo Lacão diz que "há muito trabalho a fazer" na cibersegurança.

Fábio Nunes
fnunes@medianove.com

A importância da cibersegurança é atualmente inquestionável. Vivemos num mundo no qual o peso do digital é cada vez maior e esse peso só vai aumentar. Os desafios que a tecnologia, que segue num caminho de constante e rápida evolução, vai impor serão vários, motivo pelo qual a cibersegurança terá de acompanhar essa evolução e responder às necessidades de pessoas e organizações.

Em declarações ao Jornal Económico, Arlindo Oliveira defende que a cibersegurança "é absolutamente essencial em todas as áreas da sociedade", seja nas infraestruturas informáticas, no sistema financeiro, no sistema de distribuição, no sistema energético, ou no sistema de justiça. O professor do Instituto Superior Técnico e presidente do INESC frisa que neste mundo digital a "ameaça grave a uma rede de computadores pode paralisar uma economia". "Provavelmente é uma das questões mais importantes do mundo tecnológico atual, garantir a segurança a contra-ataques informáticos de *hackers* e de agentes hostis", diz.

Tal como Arlindo Oliveira, também Paulo Lacão considera que a importância da cibersegurança é "enorme". "Numa sociedade e numa economia crescentemente digitalizada e dependente de sistemas de informação, a resiliência, a segurança e a integridade desses sistemas torna-se fundamental para o funcionamento da sociedade. O que antes não estava dependente desses sistemas, hoje, e cada vez mais, tende a ficar dependente desses sistemas", afirma o advogado e consultor sénior na Melo Alves, especialista nos temas da cibersegurança e da privacidade e proteção de dados. Paulo Lacão constata que atualmente assistimos a um movimento de digitalização em todos os sectores da atividade económica, o que torna imperativo ter uma boa capacidade de proteção. "Todos os valores, quer a nível pessoal, de defesa da esfera pessoal, da intimidade, quer a nível das empresas e da salvaguarda dos seus bens económicos, estão e ficarão crescentemente dependentes da capacidade de se assegurar a segurança dos sistemas de informação".

Arlindo Oliveira
Professor do Instituto Superior Técnico e presidente do INESC

Paulo Lacão
Consultor sénior na Melo Alves, especialista em cibersegurança

Impacto da IA

A inteligência artificial representa um desafio acrescido no campo da cibersegurança. A tecnologia está a ser cada vez mais utilizada e tem progredido a uma velocidade vertiginosa. "Acho difícil de prever o impacto, mas ninguém duvida que vai ser absolutamente disruptivo e transformador. Vai ter impacto sobre o indivíduo, sobre a proteção da pessoa e vai até suscitar novas formas de lesão de bens pessoais que antes da inteligência artificial não se imaginavam, como, por exemplo, a criação dos *deepfakes* (...) Do ponto de vista da cibersegurança, também terá impacto porque cada vez mais é possível conceber formas de intrusão mais sofisticadas e é necessário haver capacidade de conceber uma resposta a essas novas formas de lesão", sublinha Paulo Lacão.

Já o presidente do INESC argumenta que a inteligência artificial "vai ter várias dimensões". "Há uma preocupação muito grande que a inteligência artificial possa ser usada para simular ataques, no caso particular da cibersegurança. Para simular mensagens que parecem verdadeiras, para simular vídeo, chamadas telefónicas.

A falsificação usando conteúdos criados sinteticamente em grande escala é uma das preocupações. Depois, também se pode usar a inteligên-

A difusão e a utilização cada vez mais frequente da inteligência artificial representam um desafio acrescido. As pessoas e as organizações podem ficar mais vulneráveis face à evolução desta tecnologia

cia artificial para outros tipos de engenharia social, mas também para identificar fragilidades em sistemas. Da mesma forma que um *hacker* percorre sistemas operativos à procura de fragilidades em sistemas, isso pode ser programado para ser feito pela inteligência artificial", explica Arlindo Oliveira. "São duas formas óbvias nas quais um *hacker* ou um atacante pode utilizar a inteligência artificial para tornar mais eficiente o seu trabalho. De uma forma, está a fazer o mesmo que as outras pessoas fazem, mas como ele está no lado negro da Força, torna isto mais perigoso (...) A inteligência artificial pode dar uma escala e uma flexibilidade a um atacante que até agora não existia ou, pelo menos, era mais difícil de conseguir", acrescenta.

No entanto, o professor catedrático apressa-se a referir que a inteligência artificial é uma tecnologia de "duplo uso, no sentido em que pode ser utilizada para atacar e para defender". "É preciso dizer que a inteligência artificial pode ser utilizada do lado bom. Da mesma forma que a inteligência artificial pode ser utilizada para identificar fragilidades em sistemas, também pode ser utilizada para corrigir essas fragilidades, pode ser utilizada para identificar padrões que correspondam a ataques, e pode ser usada para identificar mensagens falsas nas redes sociais", exemplificou.

O panorama em Portugal

Questionados sobre a evolução registada por Portugal em termos de cibersegurança, Arlindo Oliveira diz ter "a sensação de que o Centro Nacional de Cibersegurança, as instituições oficiais e as empresas, estão ao nível de padrões internacionais". Paulo Lacão refere que "tem havido uma crescente consciencialização dos problemas de cibersegurança, dos quais já se fala há imenso tempo", mas acha que se vai "sentindo de uma forma cada vez mais efetiva a necessidade real, ou a existência real desses problemas, na vida concreta das empresas e na experiência individual das pessoas". Contudo, assinala que "ainda há muito trabalho a fazer para assegurar níveis de segurança, de resiliência e de integridade elevados na economia portuguesa, em geral". "Acho que a generalidade das empresas, tendo consciência de que o problema existe, não tem muitas capacidades nem conhecimentos técnicos para efetivamente adotar as medidas que se impõem. Muitas vezes também há uma grande dependência das empresas prestadoras de serviços, e pode não haver uma melhor gestão na forma como a empresa está aberta a terceiros e se expõe", indica.

Cibersegurança, Inteligência Artificial e colaboração

Maria Antónia Saldanha
Country Manager da Mastercard Portugal

A complexidade das ameaças à cibersegurança está a exigir às organizações públicas e privadas e, sobretudo, às entidades gestoras de infraestruturas críticas, abordagens cada vez mais complexas à proteção dos seus ativos digitais. É assim, também, na indústria de pagamentos, que tem estado na vanguarda do combate às ameaças à integridade dos sistemas e dos dados das transações, através de estratégias inovadoras que poderão servir de modelo para outros sectores.

Na verdade, o nosso compromisso com a cibersegurança passa, também, por impulsionarmos novas ideias e novas abordagens para salvaguardar um ecossistema em evolução - do físico ao digital, ao metaverso e a todas as interações que os caracterizam. São exemplo disso as iniciativas que temos implementado ao longo dos últimos meses e que mostram a abordagem multifacetada, que aproveita a inteligência artificial (IA), colaborações com outros setores e medidas proativas para proteger todos os participantes no cenário dos pagamentos digitais.

A IA está, alías, no centro da estratégia de cibersegurança da Mastercard. As ferramentas baseadas em IA que introduzimos no nosso portfolio, como o Cyber Shield e sistemas de prevenção de fraudes em pagamentos em tempo real, que utilizam machine learning para detetar e responder a anomalias nos padrões de transação de forma mais eficiente do que os métodos tradicionais. Estas tecnologias representam um avanço significativo na cibersegurança preditiva, oferecendo uma resposta ágil a potenciais ameaças antes que se manifestem em violações.

Além da implantação de tecnologia, a Mastercard também é pioneira em esforços colaborativos. Reconhecendo que a cibersegurança não é um desafio para ser enfrentado isoladamente, a Mastercard uniu forças com entidades como a Feedzai para melhorar a proteção contra fraudes em campos emergentes como as criptomoedas. Esta parceria não só fortalece os mecanismos de defesa contra fraudes relacionadas com criptomoedas, mas também garante um ambiente mais seguro para a adoção de novas tecnologias financeiras.

Mas a abordagem da Mastercard vai além da tecnologia e da colaboração. Estamos, também, profundamente envolvidos na promoção de talentos na área da cibersegurança. O nosso conceito inovador de "ciber atletas", que competem e melhoram os seus skills em ambientes simulados, é uma abordagem inovadora para colmatar a lacuna de competências em cibersegurança. Ao tornar o setor mais acessível e envolvente, a Mastercard está a contribuir para garantir um fluxo constante de profissionais qualificados, prontos para enfrentarem os desafios de cibersegurança do futuro.

Noutro domínio muito relevante para a economia, a Mastercard desenvolveu um conjunto de medidas proativas fundamentais para combater a chamada "fraude amigável" e aumentar a transparência das transações, sobretudo para as pequenas empresas, que têm na gestão de reclamações e reembolsos um verdadeiro quebra-cabeças. Em causa está a necessidade de proteger os interesses financeiros dos clientes, mas também a importância de incutir um maior sentimento de confiança e segurança nas transações digitais.

A abordagem proativa e multifatorial da Mastercard à cibersegurança estabelece uma referência na indústria dos pagamentos. Ao dar prioridade às tecnologias avançadas de IA, de promover a colaboração e estimular novos talentos, a Mastercard não está apenas a responder às ameaças à cibersegurança, mas está, também, a moldar ativamente um futuro mais seguro para a economia digital.

À medida que navegamos rumo à Next Economy, vemos a cibersegurança como um desafio que abre oportunidades para inovar e liderar a transformação digital no sector financeiro e na indústria dos pagamentos.

com o apoio