manchete

Jornal Económico
Suplemento
28-12-2018

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 10000
Temática: Tecnologia
Dimensão: 1153 cm²
Imagem: S/Cor
Página (s): 4

PROTEÇAO CONTRA AMEAÇAS

Cibersegurança deve fazer parte do ADN das empresas

As organizações investem cada vez mais em tecnologias emergentes como parte dos seus programas de transformação digital.

ANTÓNIO SARMENTO
asarmento@jornaleconomico.pt

A crescente dependência relativamente à tecnologia faz com que o tema da Cibersegurança tenha que assumir outra relevância, na medida em que a sua inexistência põe em causa direitos básicos individuais e coletivos – como a privacidade, o crescimento económico e a própria democracia. "A primeira preocupação deve ser garantir uma abordagem holística ao tema da segurança digital, assegurando que a resposta à sofisticação crescente das ameaças, decorrente de um contexto cada vez mais complexo, tem uma resposta que salvaguarda todas as múltiplas vertentes da segurança – desde a identidade, passando pelos dispositivos e aplicações e terminando na própria informação.

Em segundo lugar, teremos que ter em consideração que a escala do problema pressupõe igualmente uma resposta com meios adequados, tipicamente apenas suscetíveis de encontrar recorrendo a serviços *cloud*. É hoje claro que o volume de dados a processar e a capacidade computacional necessária para detetar, avaliar e responder às ciberameaças implicam uma resposta tecnológica só alcançável via serviços *cloud*.

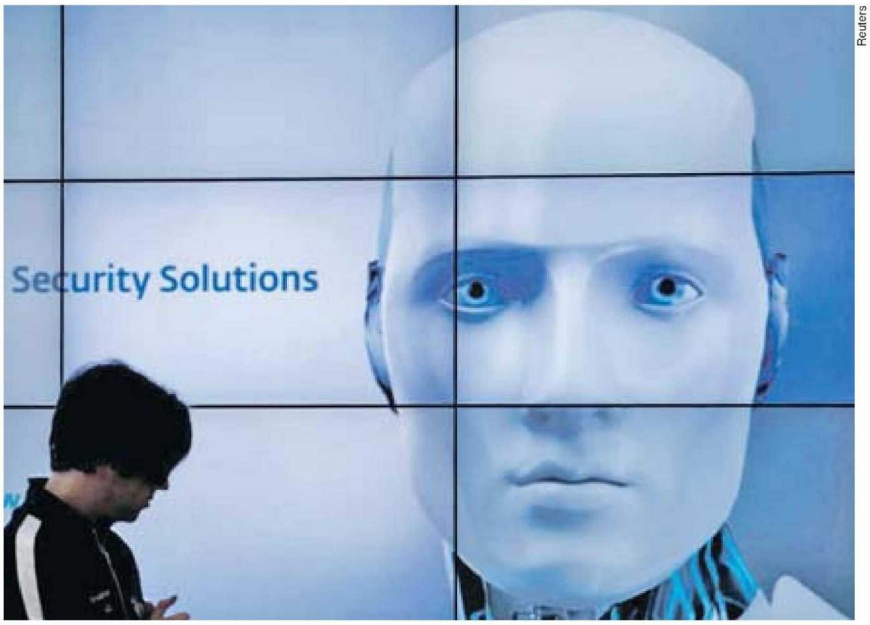
Em terceiro lugar, teremos que destacar o papel que a Inteligência Artificial pode e deve desempenhar na resposta ao cibercrime, analisando informação em escala, identificando padrões, prevendo riscos e ameaças, eliminando ataques e vulnerabilidades e automatizando processos. Finalmente, destacaria a importância da cooperação entre os vários protagonistas do ecossistema, seja por via de parcerias entre empresas privadas, mas igualmente pela colaboração estreita com entidades públicas e governos, fazendo da Cibersegurança um desígnio coletivo e global", explica André Aragão Azevedo – Diretor Nacional de Tecnologia da Microsoft Portugal.

Um ano após várias organizações terem sido abaladas por uma série de falhas de cibersegurança de grande escala e numa altura em que se fala frequentemente de ciberataques patrocinadas por estados, o estudo EY Global Information Security Survey 2018-19 (GISS) *Is cybersecurity about more than protection?*, revela que a cibersegurança continua a ganhar cada vez mais importância na agenda dos decisores.

"As organizações investem cada vez mais em tecnologias emergentes como parte dos seus programas de transformação digital, e muito embora esses programas tenham criado várias nova possibilidades, foram também responsáveis por novas vulnerabilidades e ameaças. As organizações devem ter presente que a construção de um sólido nível de segurança com os seus clientes é algo crítico para o sucesso dos seus programas de transformação. Para alcançar esta confiança, é necessário que a cibersegurança faça parte do ADN da organização, algo que começa com a sua inclusão na estratégia de negócio", refere Sérgio Martins, associate partner da EY.

"A Cibersegurança deixou de ser uma boa prática, hoje em dia é uma obrigação legal para a maioria das empresas. As principais obrigações estão no Regulamento Geral de Proteção de Dados (RGPD) e na Diretiva NIS (transposta em Portugal pela Lei nº 46/2018). As empresas estão obrigadas a garantir a segurança da sua informação e dos seus sistemas de informação. Para algumas empresas – os operadores de serviços essenciais – há obrigações acrescidas, que pretendem garantir a segurança do próprio ecossistema", acrescenta Daniel Reis, sócio da PLMJ e coordenador da equipa de TMT (Telecomunicações, Media e Tecnologias de Informação).

Sobre como é que as empresas podem otimizar as ferramentas de cibersegurança é fundamental a existência de uma plataforma tecnológica que lhes garanta o nível de segurança e de conformidade adequado. O nível de investimento que uma empresa terá que fazer para responder de forma autónoma a este desafio ultrapassa a capacidade financeira da esmagadora maioria das organizações. "Por este motivo, o recurso a soluções externas de parceiros tecnológicos como a Microsoft, que disponibilizam soluções de fácil implementação e que garantem o cumprimento de base de requisitos de segurança e de conformidade, pode ser uma opção. Os serviços de *cloud* em híper escala permitem hoje beneficiar de uma abordagem de segurança integrada que contempla as múltiplas dimensões do problema (segurança de identidade, dispositivos, aplicações e dados), e as ferramentas de controlo e reação que as organizações necessitam", conclui André Aragão Azevedo.



Reuters


ANDRÉ ARAGÃO AZEVEDO
Diretor Tecnologia Microsoft


SÉRGIO MARTINS
Associated partner EY


DANIEL REIS
Sócio da PLMJ

OS NOVOS CONCEITOS DE SEGURANÇA

Para Daniel Reis, sócio da PLMJ e coordenador da equipa de TMT (Telecomunicações, Media e Tecnologias de Informação), o novo Regulamento Geral de Proteção de Dados (RGPD) trouxe "uma obrigação de garantir a segurança dos dados pessoais tratados pela empresa". Para o advogado, o RGPD introduz conceitos de segurança de informação na legislação. O célebre artigo 32 determina que quem trata dados pessoais está obrigado a aplicar medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, que incluem:

- Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.