manchete

Jornal Económico

21-12-2018

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 10000
Temática: Tecnologia
Dimensão: 761 cm²
Imagem: S/Cor
Página (s): 26/27

TECNOLOGIA

"Cibersegurança é 'enabler' das empresas e não custo"

Frederico Macias, 'associate partner' da Deloitte, acredita que o investimento na prevenção de ataques informáticos pode ter retorno.

MARIANA BANDEIRA
mbandeira@jornaleconomico.pt

Depois de ter estado uma década na Deloitte, entre 2003 e 2013, Frederico Macias regressou este ano à consultora para prestar serviços de consultoria de gestão na área de risco. O *associate partner* afirma que regressa "a casa" para um "desafio diferente". Na mala trouxe a missão de fazer com que as empresas passem a ver a cibersegurança como valor acrescentado na sua estratégia de digitalização e mudem a forma como olham para o investimento na mesma, que, na sua opinião, tem retorno.

"A cibersegurança deve ser vista como um *enabler* da performance das empresas e não só do ponto de vista do custo. Muitas vezes, as pessoas não contabilizam a ineficiência que é criada nas organizações com os ataques de *phishing* que existem e levam tempo a perceber o que são", explica o responsável pela equipa de cibersegurança ao Jornal Económico.

Frederico Macias refere que algumas empresas gostam de um produto tecnológico, investem nele, mas não fazem o seu enquadramento numa estratégia global e sustentada. Para prevenir más decisões (e *hackers*), o antigo diretor de IT do grupo Sovena deixa vários conselhos: avaliar o risco do perfil de negócio; avaliar os ativos quantitativa e qualitativamente; avaliar a automaturidade em cibersegurança e desenhar um *roadmap* "para que possa fazer um caminho sustentado no tempo e m vez de investir de forma isolada em tecnologia".

Na entrevista ao JE, o *associate partner* realçou também que a oferta formativa na Europa vai continuar a crescer, mas o acréscimo será maior nos Estados Unidos, nomeadamente em universidades de renome como a Carnegie Mellon e o MIT. Além disso, considera que as oportunidades de emprego também serão maiores e que os profissionais com bom enquadramento da atuação e do histórico da empresa serão os mais requisitados para postos de trabalho em cibersegurança. "As pessoas vão continuar a ser uma parte muito importante na resposta aos ciberataques. Tipicamente, envolve uma análise de impacto nas áreas de negócio, falar com os *owners* dos ativos, o que não é algo que se consiga fazer de forma totalmente autónoma com a tecnologia", argumenta o porta-voz da consultora em Portugal, cujos especialistas têm desenvolvido projetos com o Centro Global de Operações de Cibersegurança da Deloitte EMEA, em Madrid.

O risco também pode ser antecipado com tecnologias de *user behavior analytics*, que têm detetado cada vez mais padrões anómalos no comportamento dos utilizadores. Inclusive, por exemplo, ficar de 'olho' no funcionário que em 24 horas aumentou significativamente o volume de *downloads* de dados dentro da empresa, o que pode significar que estará de saída.

A seu ver, as empresas portuguesas já perderam "bastante" com o cibercrime, sobretudo no setor energético, saúde e banca. "São alvos apetecíveis. Nem todos os ataques são tornados públicos, mas a regulamentação mudou e tornou premente a necessidade de reportar este tipo de perdas", diz.

Empresas com mais obrigações de notificar ataques

A 13 de agosto, a Lei nº46/2018 estabeleceu o regime jurídico da segurança do ciberespaço, transpondo a diretiva europeia de 6 de julho de 2016, relativa à segurança das redes e da informação em todos os Estados-membros. O novo quadro legal estabelece que a Administração Pública, os operadores de infraestruturas críticas, prestadores de serviços digitais e essenciais têm de tomar e cumprir medidas técnicas e organizativas para gerir os riscos na segurança das redes e dos sistemas de informação. Ademais, têm de obedecer às instruções de cibersegurança emitidas pelo Centro Nacional de Cibersegurança (CNCS). Caso contrário, arriscam-se a multas entre 5.000 a 25.000 euros (pessoa singular) e 10.000 a 50.000 (pessoa coletiva).

O CNCS também prevê publicar, até ao final de março de 2019, um conjunto de normas que deverão conduzir os operadores económicos de 14 setores em matéria de cibersegurança. Esta autoridade vai, por exemplo, apresentar um "Quadro de Referência Nacional", ao qual podem aderir entidades portuguesas, públicas e privadas, cuja operação rentabilize os recursos disponíveis no ciberespaço. ●

Energia, saúde e banca são "alvos apetecíveis", acredita Frederico Macias, 'associate partner' da Deloitte

manchete

Jornal Económico

21-12-2018

Periodicidade: Semanário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 10000
Temática: Tecnologia
Dimensão: 761 cm²
Imagem: S/Cor
Página (s): 26/27