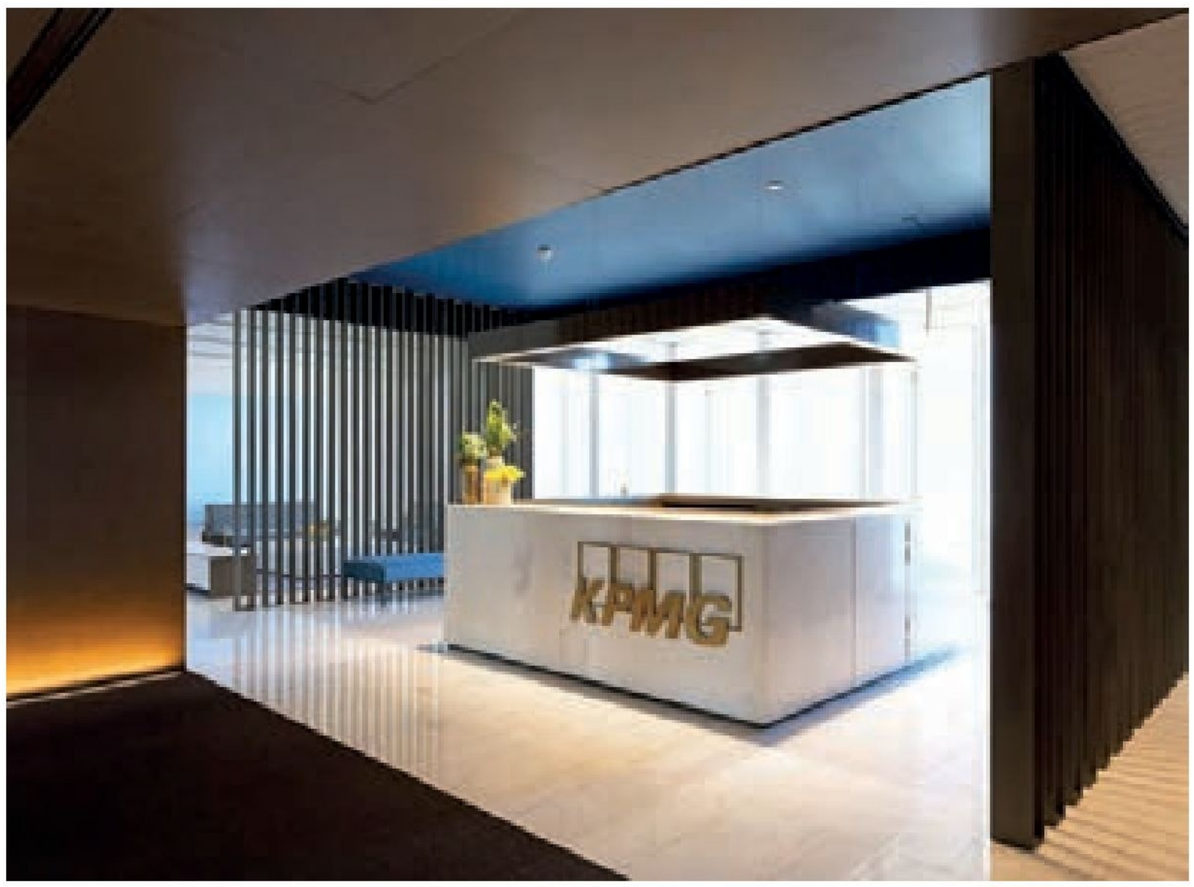
KPMG

UM MUNDO DIGITAL FIÁVEL

A KPMG TEM UMA POSIÇÃO PRIVILEGIADA PARA APOIAR AS EMPRESAS NESTE DESAFIO



A KPMG apoia os clientes na criação de um mundo digital robusto e fiável, oferecendo uma combinação de experiência tecnológica, conhecimento profundo do negócio e profissionais de excelência com uma paixão pela protecção e resiliência do negócio. Em entrevista à Executive Digest, Sérgio Martins, Partner da KPMG Portugal e responsável da área de cibersegurança, explica como as organizações se devem proteger ao nível da cibersegurança.

A Cibersegurança é um dos grandes desafios da nossa sociedade, nomeadamente, para as empresas. Que soluções é que a KPMG coloca à disposição dos clientes?

A cibersegurança está cada vez mais no topo das prioridades dos nossos clientes e na última edição do nosso estudo CEO Outlook, a cibersegurança destaca-se como um dos principais riscos para os próximos anos, ao lado de temáticas como incerteza geopolítica, alterações climáticas e aumento das taxas de juro.

Na KPMG apoiamos os nossos clientes na criação de um mundo digital robusto e fiável, oferecendo uma combinação de experiência tecnológica, conhecimento profundo do negócio e profissionais de excelência com uma paixão pela protecção e resiliência do negócio dos nossos clientes. As soluções vão desde a estratégia de governo, gestão de risco e conformidade da cibersegurança até à implementação e operação tecnológica, que inclui arquitecturas de segurança de centros de dados e Cloud, soluções de gestão de acessos e identidades, desenho de SOCs, testes de intrusão e resposta a incidentes. Pretendemos que o conjunto de serviços e soluções que disponibilizamos possa ser o mais transversal possível, de forma a ajudar a garantir uma segurança efectiva das operações dos nossos clientes.

Quais os tipos de ciberataques mais comuns que temos hoje em dia no sector empresarial português?

Tendo em conta que a internet é um meio global e os actores do cibercrime não têm fronteiras, os ataques a que temos assistido a nível nacional não diferem muito daquilo que são as tendências globais.

Assistimos a muitos ataques direccionados – Spearphising, tipicamente a pessoas de topo das empresas, onde os atacantes se fazem passar por entidades credíveis de modo a obter informação confidencial, como por exemplo as suas credenciais. Estas credenciais obtidas podem depois ser utilizadas para roubo de informação ou como porta de entrada para acederem a outros sistemas e continuarem assim a cadeia de ataque.

Os ataques de ransomware também são muito comuns, porque são um tipo de ataque que pode dar retorno financeiro imediato para os grupos de cibercrime organizado, e caso a empresa não tenha o nível de protecção e recuperação adequado, pode ficar completamente refém e ter de pagar quantias por vezes muito avultadas de forma a poder recuperar os seus dados.

Também existem alguns ataques perpetrados por Hacktivistas, que são grupos que defendem uma causa específica e que procuram

COMPETÊNCIAS

A KPMG DISPÕE DE UM CONJUNTO VASTO DE COMPETÊNCIAS QUE VAI MUITO PARA ALÉM DO CONHECIMENTO ESPECÍFICO DE CIBERSEGURANÇA, NOMEADAMENTE COMPETÊNCIAS NAS ÁREAS TECNOLÓGICA, FINANCEIRA, FISCAL, FRAUDE, ENTRE OUTRAS

exposição mediática nas suas acções de modo a promovê-la, tipicamente são ataques de negação de serviço com o objetivo de condicionar serviços online, como sites corporativos de empresas ou organismos governamentais.

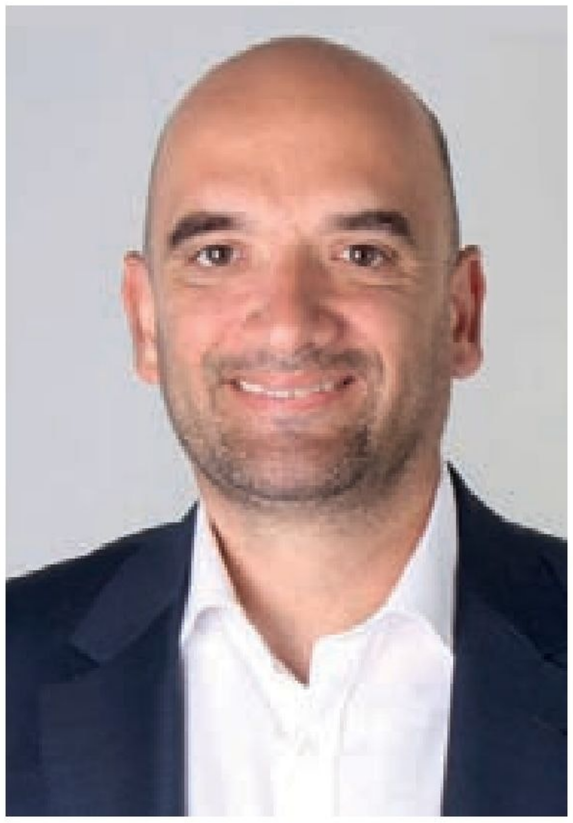
Com a utilização cada vez mais massiva da Inteligência Artificial, quais os principais desafios ao nível da protecção de dados?

A adopção massiva de Inteligência Artificial pode ser analisada como uma faca de dois gumes. Por um lado, permite à comunidade de cibersegurança, e especificamente às empresas, terem acesso a tecnologias de detecção e prevenção de ataques mais sofisticadas, e um exemplo claro disso são os centros de operação de cibersegurança onde a Inteligência artificial pode ajudar na detecção de ataques e até automatizar alguns tipos de resposta num modo 24/7, assim como libertar os operadores humanos para outro tipo de actividades.

Por outro lado, os actores do cibercrime também já estão a recorrer à inteligência artificial para se munirem de técnicas de ataque mais complexas e estão a utilizar esta tecnologia para automatizar campanhas de phishing, criar imagens e vídeos deepfake para engenharia social e desenvolver código malicioso que seja mais evasivo à deteção.

Estamos a viver uma fase de grande transformação com a introdução de Inteligência artificial na sociedade e ainda ninguém sabe efectivamente qual vai ser a forma e a extensão do impacto que vai ter, pelo que a melhor maneira de nos prepararmos é apostar no conhecimento das equipas de cibersegurança e na criação de um ecossistema de colaboração com universidades, instituições públicas e empresas.

A CIBERSEGURANÇA ESTÁ CADA VEZ MAIS NO TOPO DAS PRIORIDADES DOS NOSSOS CLIENTES



» Sérgio Martins, Partner da KPMG Portugal

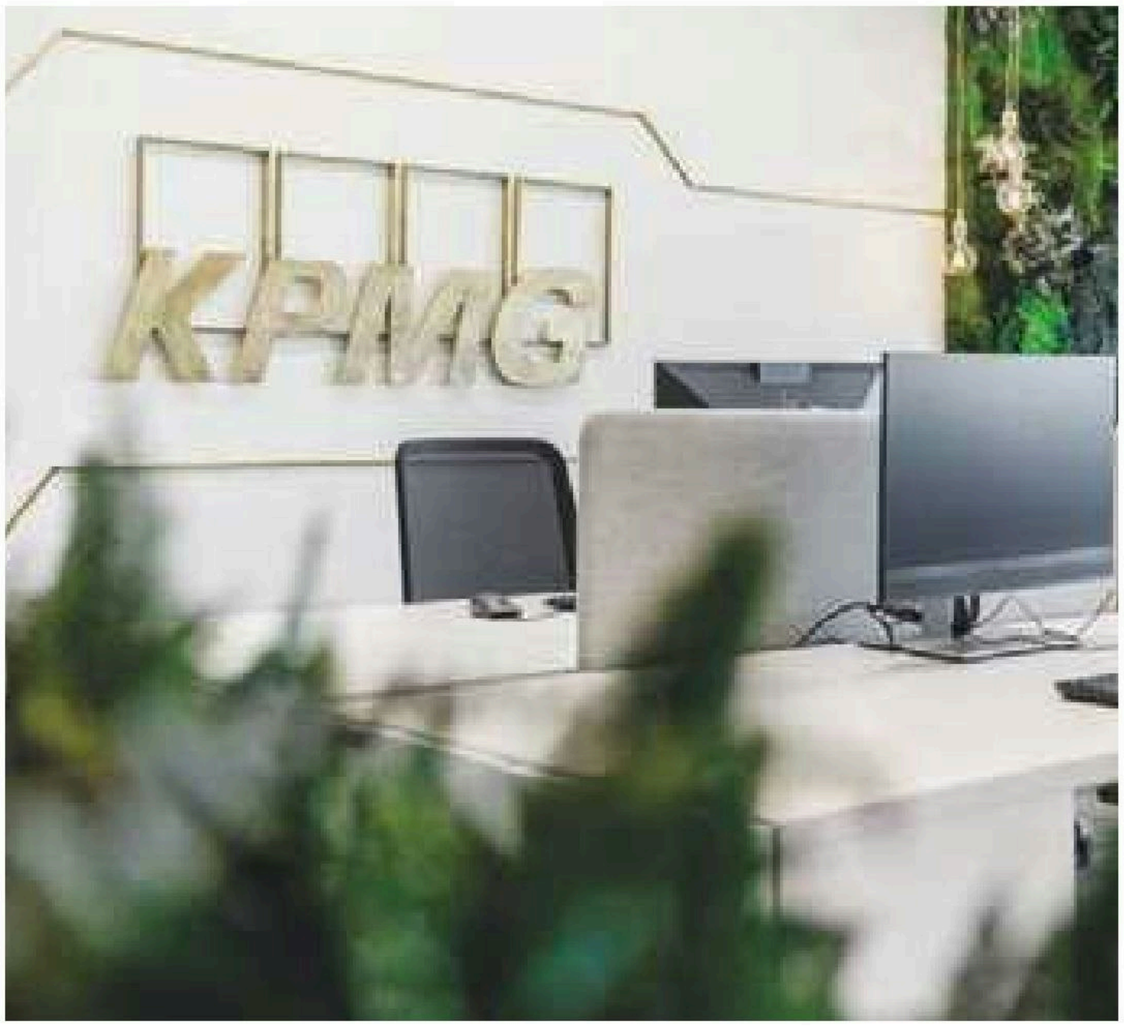
Como é que a KPMG pode ser o parceiro ideal das empresas na adoção de soluções de segurança?

A KPMG tem uma posição privilegiada para apoiar as empresas neste desafio porque como empresa multidisciplinar, dispõe de um conjunto vasto de competências que vai muito para além do conhecimento específico de cibersegurança, nomeadamente competências na área tecnológica, financeira, fiscal, fraude, estratégia e operações. Esta multidisciplinariedade permite-nos ter uma visão clara do negócio dos nossos clientes e adequar a estratégia de cibersegurança ao negócio. Outro diferenciador é a escala global da rede KPMG: hoje somos mais de 9000 profissionais em cibersegurança em todo o mundo e trabalhamos em conjunto, sendo muito comum incluirmos profissionais de outros países nos projectos da KPMG em Portugal, bem como os profissionais portugueses participarem em projectos internacionais. Isto cria um ambiente de partilha e crescimento rápido que se reflecte na forma como abordamos os desafios dos nossos clientes, com a inclusão de aceleradores e ferramentas globais.

Consideram que as empresas portuguesas estão bem preparadas para estes desafios?

As empresas portuguesas têm feito um investimento crescente em cibersegurança, no entanto esta é uma jornada contínua, o panorama de ameaças está sempre a mudar com novos tipos de ataque, pelo que é necessário continuar o investimento para manter e melhorar os níveis de maturidade e resiliência das empresas.

No meu entender o mercado nacional tem um grande desafio, que é a escassez de talento na área de cibersegurança, e as pessoas são o ingrediente chave para uma postura de segurança forte.



Existe uma falta reconhecida de profissionais de cibersegurança em todo o mundo e Portugal não é excepção. Em termos de oferta Portugal até já tem cursos de STEM, Pós-graduações e Mestrados especializados em cibersegurança, no entanto a procura interna e externa é bastante superior. Os muitos profissionais que emigraram durante a crise, as Nearshores com os seus centros de cibersegurança instaladas em Portugal, a competição natural por talento entre empresas em Portugal e mais recentemente a proliferação do trabalho remoto para empresas no estrangeiro está a causar uma grande pressão na captação e retenção de talento pelas empresas portuguesas nesta área. As empresas têm de ser muito criativas na forma como gerem e mantêm o talento motivado, sabendo de antemão que é muito difícil competir financeiramente contra projectos internacionais.

A KPMG PORTUGAL FEZ RECENTEMENTE UM GRANDE REFORÇO NA EQUIPA DE CIBERSEGURANÇA, COM A CONTRATAÇÃO DE MAIS DE 20 PROFISSIONAIS ALTAMENTE ESPECIALIZADOS

Ao fazerem parte de um mundo conectado, as organizações estão expostas a um maior número de ameaças. Como é que as empresas se podem proteger?

Em termos de prioridades considero que o mais relevante seja criar uma higiénica básica de segurança. Está provado estatisticamente que a grande maioria dos ataques bem-sucedidos são realizados explorando vulnerabilidades muito básicas, como emails de phishing para obtenção de credenciais a colaboradores desatentos; exploração de vulnerabilidades que já são conhecidas há algum tempo mas onde os sistemas ainda não foram actualizados; acessos a sistemas que foram deixados com as passwords de base ou com palavras chave muito fracas, etc. Ou seja, se conseguirmos ter dentro da organização uma boa higiene de segurança que garanta que os controlos básicos estão implementados conseguimos reduzir a nossa superfície de ataque drasticamente. Depois disto é importante ir investindo gradualmente na capacidade de protecção contra ameaças mais avançadas, sempre com uma visão de gestão de risco, até termos um nível de cibersegurança adequado.

Também é muito importante ter a noção de que por mais que se invista em cibersegurança, ninguém está 100% seguro e existe sempre um risco residual de sermos atacados. Nesse sentido, para além de investir na prevenção e protecção é fundamental estar preparado para a recuperação, caso o ataque seja bem sucedido, de forma a termos a capacidade de recuperar a informação que suporta o negócio em tempo útil e gerir eventuais impactos reputacionais e financeiros que daí advenham.

Ao nível da cibersegurança, como é que a KPMG olha para 2024?

A KPMG Portugal fez recentemente um grande reforço na equipa de cibersegurança, com a contratação de mais de 20 profissionais altamente especializados, sendo que em Setembro inaugurámos o nosso Hub Tecnológico de Évora, onde já começaram a ser contratados os primeiros profissionais de cibersegurança. Neste momento temos cerca de 40 profissionais espalhados pelos nossos escritórios de Lisboa, Porto e Évora, o que nos vai permitir continuar a apoiar de forma eficaz os nosso clientes. Em 2024 prevemos que o número de incidentes de cibersegurança continue a aumentar, com especial destaque para o incremento de ataques à internet das coisas – IoT, ataques suportados por inteligência artificial, ataques a redes 5G e provavelmente o tema dos ataques criptográficos utilizando computação quântica vai ganhar relevância. Também será de esperar a emergência de novas regulamentações de cibersegurança a nível europeu e nacional, bem como de reguladores em sectores específicos. Serão tempos desafiantes, mas com uma abordagem bem definida as organizações mais fortes neste capítulo vão certamente poder tirar vantagens competitivas. ●