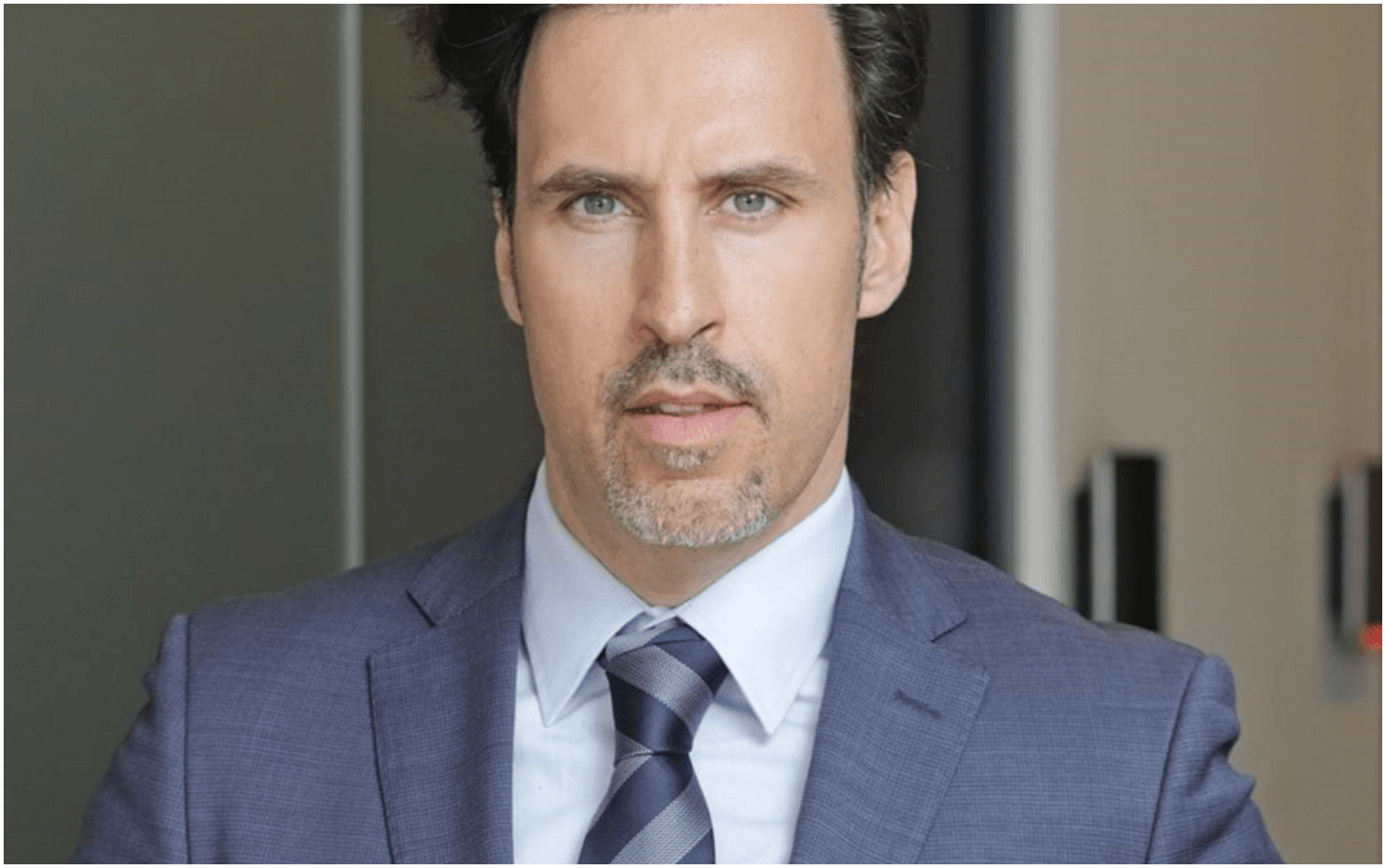
CEO da VisionWare sobre a cibersegurança em Portugal: “O caso da Vodafone constituiu o grande ‘turning point’”

jornaldenegocios.pt/empresas/tecnologias/detalhe/ceo-da-visionware-sobre-a-ciberseguranca-em-portugal-o-caso-da-vodafone-constituiu-o-grande-turning-point



Bruno Castro, fundador e CEO da VisionWare.

"O ciberataque à Vodafone em fevereiro de 2022 e os ciberataques registados nos meses seguintes em Portugal e pelo mundo fora, revelaram uma procura extremada por serviços de cibersegurança", afirma Bruno Castro, fundador e CEO da VisionWare, tecnológica portuguesa especializada em cibersegurança e segurança de informação, que emprega 105 pessoas e fechou 2023 com uma faturação de 4,6 milhões de euros.

Qual é o estado de Portugal em matéria de cibersegurança, no que se refere a programas de prevenção e adoção de medidas, e na prevenção de ciberataques por parte do tecido empresarial português?

Apesar dos esforços do Governo português e da maior atenção e sensibilização da sociedade civil atual, os ciberataques continuam a ser uma grande preocupação no país. Parece-me cada vez mais evidente que a ameaça representada pelos cibercriminosos está a crescer e que é necessário fazer mais para prevenir acontecimentos futuros.

Como tal, Portugal precisa de continuar a reforçar as suas infraestruturas de cibersegurança e a desenvolver estratégias eficazes para proteger os seus cidadãos, empresas e infraestruturas contra o número crescente de ciberataques, oriundos de redes criminosas diversas, cada vez mais bem organizadas e com uma maior capacidade disruptiva.

Face ao incremento quase explosivo do número de ciberataques, infelizmente, as autoridades não dispõem de recursos necessários para responder a todas as solicitações. Para além de mais ataques, e com maior taxa de sucesso, são também cada vez mais complexos e sofisticados, e, portanto, obrigam a um esforço muito superior no processo da sua e investigação.

Seguir o rasto da pegada digital deste tipo de grupos criminosos, que atuam de forma encoberta, prolongada no tempo, e tecnicamente aprimorada, é cada vez mais exigente – tecnologicamente, na capacidade de resposta e conhecimento especializado envolvido - para quem tenta investigar e prevenir este tipo de ciberataques.

As autoridades competentes estão perante um enorme desafio, que, para além da capacidade de resposta, ainda se prende com o binómio técnico vs "know how" especializado.

Então, o que é que se deve fazer?

A aposta terá de ser sempre pela via da crescente literacia e formação/sensibilização de todos os cidadãos, independentemente da sua função/cargo, visto que, qualquer um de nós poderá ser vítima de um ataque malicioso ou fraudulento, já que o fator humano continua a ser um dos grandes responsáveis pela consumação das ameaças.

E qual deve ser o papel do Estado?

O Estado e a Administração Pública e demais organismos estatais deverão ser os primeiros a preconizar e implementar medidas de segurança diárias e fazer respeitar as demais normas e diretivas nacionais e internacionais, com vista ao cumprimento de uma maior segurança cibernética. A cibersegurança constitui aliás, um dos componentes indispensáveis face à conformidade com a lei da proteção e privacidade de dados.

Aproveitando o Plano de Recuperação e Resiliência (PRR)…

A meu ver, o PRR confere uma oportunidade única de transformação digital e de crescente capacitação a este nível, pelo que há que saber aproveitar, para que possamos tirar o máximo partido do potencial associado à economia dos dados. Deverá ainda ser acautelado um plano de contingência em caso de violação de segurança que defina as medidas de eliminação/mitigação de riscos, procedimentos a adotar, comunicação à Comissão Nacional de Proteção de Dados (CNPD) e informação aos demais titulares dos dados.

Em complemento, os SMD – Selos de Maturidade Digital – vêm complementar a oferta de certificações existente, disponibilizando mais opções, com o objetivo de conferir robustez para as empresas, particularmente para as PME – que constituem grande parte do tecido empresarial em Portugal –, para que se certifiquem e para impulsionar a sua transformação e capacitação digital.

Os SMD concretizam aliás, uma das medidas do Plano de Ação para a Transição Digital, que integra o plano de ação Portugal Digital, visando a transformação digital das organizações e da economia em Portugal. O Centro Nacional de Cibersegurança (CNCS) é também um importante parceiro desta iniciativa, o que reforça a importância desta distinção. Em outubro de 2023, a VisionWare, foi a primeira empresa especializada em cibersegurança a alcançar esta distinção com a certificação Ouro, na categoria Cibersegurança. A categoria de Cibersegurança, em particular, sela o compromisso das organizações com a adoção de um guião para o processo de transição digital.

Quais são as principais tendências e ciberameaças para 2024?

Entre as possíveis tendências relacionadas ao cibercrime e às principais ameaças à segurança mundial em 2024, saliento, desde já, a clara ascensão dos ataques impulsionados via Inteligência Artificial (IA), cada vez mais sofisticados e difíceis de serem detetados e mitigados; a proliferação/banalização de "deepfakes" e manipulação dos media, com implicações sérias para a segurança cibernética e a confiança pública – veja-se o caso, por exemplo, de "deepfakes" utilizados até em campanhas políticas, nas quais Portugal estará envolvido já em março próximo;

Ataques de "ransomware" aprimorados por IA, os quais podem beneficiar do uso de algoritmos de IA para identificar alvos cada vez mais valiosos, e, em simultâneo, otimizar as suas táticas de infiltração; ataques a dispositivos IoT (Internet das Coisas); esquemas de falsificação de identidade avançada através de IA, com a criação de identidades falsas mais convincentes, dificultando assim a deteção de atividades fraudulentas; o aumento exponencial de ataques de engenharia social, em específico, o "spear phishing", isto é, ataques direcionados a um alvo/pessoa específica podem beneficiar-se do uso de IA para a personalização de mensagens, aumentando assim a probabilidade de sucesso;

A exploração de vulnerabilidades de IA na defesa cibernética, comprometendo a integridade e a fiabilidade de algoritmos e dos seus modelos; os ataques a infraestruturas e serviços críticos como a saúde e a educação, na medida em que os cibercriminosos procuram comprometer os sistemas de automação essenciais. Ciberataques contra setores críticos, serão mais comuns acabando por implicar sérias consequências e impacto na segurança pública; os desafios crescentes na deteção de ameaças com o desenvolvimento de malware específico e direcionado, ou seja, a deteção de ameaças pode tornar-se ainda mais difícil, exigindo soluções de segurança mais avançadas e robustas;

E, por último, a criação de regulamentações e leis de proteção de dados mais rigorosas em resposta às crescentes ameaças cibernéticas, sendo expectável que governos e organizações implementem regulamentações mais exigentes para garantir a segurança digital.

E quais são as grandes preocupações dos gestores das empresas relativamente a investimentos na área da segurança de informação?

Nestes últimos quase 20 anos de VisionWare, nunca tivemos tantas solicitações de ajuda para responder, orientar e investigar ciberataques bem-sucedidos, como agora. Estes ciberataques, desenvolvidos em vários formatos, e cada vez mais complexos, sofisticados e com elevado grau de sucesso, estão tipicamente focados no roubo de dinheiro ou de dados "valiosos", resultando de múltiplos fatores associados.

Por um lado, o cenário pandémico veio colocar mais pessoas, muitas sem formação, a viver no mundo cibernauta. Por outro, o ambiente de teletrabalho promoveu um certo descuido face às medidas de segurança, o que faz com que, todos, mesmo os mais formados, estejam "menos alerta" para eventuais ameaças ou comportamentos suspeitos.

Os níveis de maturidade de segurança variam de organização para organização, mas o fator humano é normalmente a maior fragilidade. As pessoas precisam de ser formadas para responderem a esta nova realidade e poderem novamente conviver com o mundo cibernauta, com tudo o que acarreta, de forma ponderada e responsável. Mais do que "literacia digital", há a necessidade de haver "literacia em cibersegurança".

Na VisionWare, temos vindo a registar um número avultado de solicitações de empresas, as quais começam agora a preocupar-se com a questão da segurança da informação e da cibersegurança, colocando-as no topo das suas prioridades de gestão.

O caso da Vodafone constituiu o grande "turning point" e atualmente, o "chip" e o "mindset" dos administradores das empresas, que detêm o poder de decisão, está a mudar, olhando para as soluções e serviços de cibersegurança não mais como um custo, mas antes como um investimento essencial, crítico, de modo a mitigar eventuais riscos e danos financeiros e reputacionais sem precedentes.

Em matéria de cibersegurança, qual é a chave do sucesso?

Não existem fórmulas mágicas ou uma vacina milagrosa contra ciberataques. A chave do sucesso será sempre a prevenção, e, agora, cada vez mais, a capacidade de resposta após um ciberataque com sucesso. Não me canso de reforçar este ponto. Prevenção e investimento em modelos de segurança contínuos, conhecer bem as infraestruturas, e, sobretudo, "stressar" constantemente os sistemas, isto é, efetuando testes de simulação de ciberataques à organização, procurando falhas e fragilidades, corrigindo-as de forma perseverante, de modo a "blindar" a organização contra quaisquer eventuais tentativas de (ciber) ataques. O conhecer a nossa capacidade de recuperação a um ciberataque é fundamental para a gestão de uma organização nos dias de hoje.

Os ciberataques, sendo cada mais frequentes e sofisticados, afetam empresas de todas as dimensões, em qualquer setor de atividade e em qualquer geografia. As multinacionais, por exemplo, além de possuírem mais recursos e dados valiosos, muitas vezes são os alvos preferenciais, contudo, o largo tecido PME também não está imune. Muitas vezes, essas empresas são vistas até como alvos mais fáceis devido à falta de investimento e nível de preparação em segurança cibernética.

Ataques como "ransomware", "phishing" e roubo de dados são comuns e os prejuízos financeiros e de reputação podem ser significativos e altamente negativos, sem recuperação possível, levando mesmo muitas vezes, à falência de algumas PME, as quais se revelem menos preparadas e com menor robustez financeira.

O ponto de ordem será sempre a implementação de modelos de governação de segurança para que daí se possa iniciar a gestão de risco e a respetiva evolução do nível de maturidade digital.