Cibersegurança em perigo: «Os ataques e...

lidermagazine.sapo.pt/ciberseguranca-em-perigo-os-ataques-estao-a-sofisticar-se-diz-bruno-castro-visionware

Cibersegurança em perigo: «Os ataques estão a sofisticar-se» diz Bruno Castro

A **cibersegurança já não é um luxo**, é uma **necessidade vital**. Num ambiente tecnológico onde, a cada minuto, seis utilizadores portugueses veem as suas contas pirateadas – segundo um relatório de 2024 da **Surfshark** -, proteger dados deixou de ser uma opção. Entre ataques crescentes e ameaças constantes, está em jogo não apenas a privacidade, mas a sobrevivência digital de empresas e cidadãos.

Este foi o repto do almoço e **Encontro de Conselheiros Leading Tech e Leading People**, que teve lugar na **Casa da Praia**, em Oeiras, na sexta-feira passada. **Bruno Castro, CEO da Visionware**, denunciou a gravidade da situação e o estado crítico da cibersegurança nacional. Com mais de 20 anos de experiência, o CEO alertou que é urgente inovar e **«repensar estratégias de defesa»** para proteger dados e garantir o futuro digital do país.

O crescimento das ameaças digitais

Nas palavras de Bruno Castro, a diferença substancial entre as organizações e os cibercriminosos **reside no tempo** e na capacidade de adaptação: «Têm tempo para planear e executar ataques sofisticados, enquanto nós precisamos transformar as nossas práticas e investir em formação e tecnologia para proteger os sistemas», afirmou.

O setor da **cibersegurança** sofreu uma revolução nos últimos anos, especialmente com a pandemia, que levou muitas empresas a digitalizarem-se de forma abrupta, sem preparação adequada. Isso criou um ambiente propício para o crescimento do cibercrime, que se profissionalizou e expandiu a um ritmo alarmante.

Atualmente, os ataques informáticos são realizados por redes organizadas, operando em fusos horários distintos, com elevados recursos e capacidades técnicas. Em suma, a tradicional imagem do **hacker solitário** é um mito. Hoje, o **cibercrime tornou-se uma indústria rentável**, com operações que funcionam de forma semelhante a consórcios empresariais.

Phishing: um desafio pela frente

Entre os vetores de ataque mais utilizados, o **phishing** continua a ser um dos principais. O método evoluiu para **esquemas mais sofisticados**, que vão muito além dos e-mails mal escritos e mensagens suspeitas. Hoje, **cibercriminosos** utilizam **dados reais** para simular comunicações autênticas, **explorando vulnerabilidades humanas** mais do que falhas tecnológicas.

Dessa forma, a estratégia baseia-se na exploração da confiança: um atacante consegue credenciais de um utilizador, acede ao seu servidor de e-mail e usa a sua identidade para **enganar contatos e redes profissionais**. O alvo recebe mensagens aparentemente seguras, que podem resultar em fraudes financeiras ou roubo de informação sensível.

Para Susana Soares, Managing Director da CHRLY, **«o que realmente importa é a capacitação das pessoas»**. Durante a sua intervenção, defendeu a necessidade de aproximar empresas com expertise em formação em cibersegurança daquelas mais vulneráveis a ataques digitais. O objetivo? Renato Azevedo, Head of Cybersecurity & Cloud Services da Capgemini, responde. Passa por «prevenir riscos e preparar profissionais para enfrentarem as crescentes ameaças do mundo digital».

O futuro da cibersegurança

Assim, a cibersegurança tornou-se uma prioridade global e, segundo Bruno Castro, «a tendência é que a sofisticação dos ataques continue a aumentar». Para as empresas, **a chave para o futuro está na formação contínua**, na adaptação constante e na parceria com especialistas que garantam uma defesa eficiente contra ameaças cada vez mais elaboradas.