Especialistas avisam que ciberataques em Portugal estão a aumentar e deixam seis recomendações para empresas se protegerem

jornaleconomico.pt/noticias/especialistas-avisam-que-ciberataques-em-portugal-estao-a-aumentar-e-deixam-seis-recomendacoes-para-empresas-se-protegerem-845105

9 de fevereiro de 2022

Sociedade

André Cabrita-Mendes 09 Fevereiro 2022, 08:25

Depois dos ataques à Vodafone e à Imprensa, os especialistas avisam que os ataques por piratas informáticos estão a aumentar em Portugal.

Os ciberataques em Portugal estão a aumentar, alertam dois especialistas em segurança digital. Depois dos ataques à Impresa e Vodafone, que se tornaram mediáticos pela forma como afetaram os serviços de duas das maiores empresas do país nos seus sectores, estes especialistas deixam várias recomendações às empresas para se protegerem.

“Num dos relatórios mais recentes da Check Point, demos nota de que o número de ciberataques contra empresas nacionais aumentou em 81% comparado com 2020. Sabemos ainda que, especificamente no setor das comunicações, a média semanal de

ataques por organização foi de 1306, sendo o quinto setor mais atacado de todos em Portugal", aponta Rui Duro da Check Point Software Technologies.

Já Bruno Castro da Visionware responde que a "realidade tem vindo a mudar nos últimos dois anos, coincidente com a pandemia – também cibernética que estamos todos a viver, e veio trazer um incremento substancial do número de ciberataques, mas especialmente, do incremento da taxa de sucesso dos ciberataques ocorridos nestes últimos dois anos. Também podemos acrescentar que os ciberataques têm sido cada vez mais disruptivos, violentos e mediáticos com um impacto financeiro/institucional cada vez maior".

– Quais as precauções que as empresas devem tomar?

Rui Duro da Check Point Software Technologies deixa várias recomendações:

– "Sensibilizar as equipas de toda a organização para práticas de cibersegurança (investir em formação). Grande parte dos ciberataques tem origem na falha humana. Consciencializar para o perigo de clicar num link ou anexo desconhecido pode fazer a diferença entre sofrer um ataque ou não";

– "Implementar soluções anti-phishing que protejam a navegação web e o correio eletrónico";

– "Realizar backups de dados de forma regular";

– "Manter os sistemas atualizados a todos os momentos. Cada atualização comporta por norma resoluções de vulnerabilidades existentes. Quanto mais desatualizado estiverem os softwares, maior é o risco de termos a segurança dos nossos sistemas comprometida";

– "Proteger a cloud, os dispositivos móveis, as redes, com soluções especializadas é igualmente crucial. Felizmente, hoje, temos soluções para empresas de todas as dimensões. Há que relembrar de que a cibersegurança não é um custo, mas um investimento que, no final do dia, pode salvar a nossa empresa".

Já Bruno Castro da Visionware aconselha as empresas a avaliarem a fazerem uma autoavaliação:

– "É cada vez mais importante as empresas e organizações/instituições – incluindo os Estados – de se auto-avaliarem regularmente no sentido de conhecerem as suas maiores vulnerabilidades e assim poderem investir esforços no sentido de as mitigarem ou simplesmente (se possível) removerem-nas. É muito comum aparecerem empresas que, durante um violento ataque não conhecerem sequer a globalidade da sua infraestrutura tecnológica ou aplicacional, quanto mais as suas vulnerabilidades. Tipicamente, essa análise é realizada muitas vezes – quando não uma maturidade adequada – no decorrer da resposta ao ciberataque".

Sobre a atuação das autoridades policiais e judiciais nestes casos, os dois especialistas concordam que a prevenção é essencial.

“A tónica deve estar na prevenção e não tanto na resolução posterior, isto é, quando o ciberataque já aconteceu. Até porque o raio de ação quando o mal está feito é naturalmente diminuto. As autoridades judiciais fazem o que lhes compete na averiguação dos danos causados e na identificação do rasto de ataque. Ainda assim, não nos podemos esquecer que a cibersegurança não é um tema preocupante apenas para pessoas e empresas. É premente que os governos comecem a tomar medidas a um nível macro para parar estas ameaças”, segundo Rui Duro.

Por sua vez, Bruno Castro disse “que quem tem que atuar mais e melhor são os gestores que têm responsabilidades nas empresas e nas organizações nacionais no sentido de promoverem um trabalho continuo de cibersegurança dentro das suas organizações. É cada vez mais fundamental a camada de gestão das empresas estarem alertas e perfeitamente sintonizadas com as exigências de segurança em viver no mundo digital e portanto este tema tem que ser uma prioridade de gestão. As autoridades já se esforçam imenso em responder o melhor possível ao crescimento exponencial deste tipo de ataques”.

Em relação a causas e autores para este ataque, o presidente da Visionware aponta que “neste momento não é possível conhecer em concreto quais foram os vetores de intrusão utilizados para realizar este ciberataque”.

“Contudo, face à dimensão e complexidade de uma infraestrutura como a Vodafone, diria que deverão existir várias possibilidades, desde ligações externas com parceiros ou até colaboradores, ou vulnerabilidades aplicacionais de serviços expostos para a Internet, até o ataque direcionado às pessoas que funções internas na Vodafone”, destaca Bruno Castro.

O responsável da Check Point, por seu turno, responde que “neste ponto, podemos apenas conjeturar. Suspeitamos que se trate de um ataque pensado e direcionado especificamente à infraestrutura Vodafone. Cabe à Vodafone e às autoridades esclarecerem o sucedido”.