# Ciberataques podem ser “devastadores” para as marcas

eco.sapo.pt/2023/08/07/ciberataques-podem-ser-devastadores-para-as-marcas

7 de agosto de 2023

O grupo pró-russo de cibercriminosos NoName057(16) terá atacado recentemente diversas páginas de internet espanholas. **As implicações de um ataque deste género para as marcas podem ser “devastadoras” e ditar mesmo o seu fim**. A ameaça é real, e em Portugal já afetou marcas como a Vodafone, a Impresa ou a Tap, podendo as consequências, no entanto, serem diferentes consoante a resposta de comunicação dada por parte da marca, observa **Bruno Castro, especialista em cibersegurança e análise forense e CEO da VisionWare, em entrevista por escrito ao +M.**

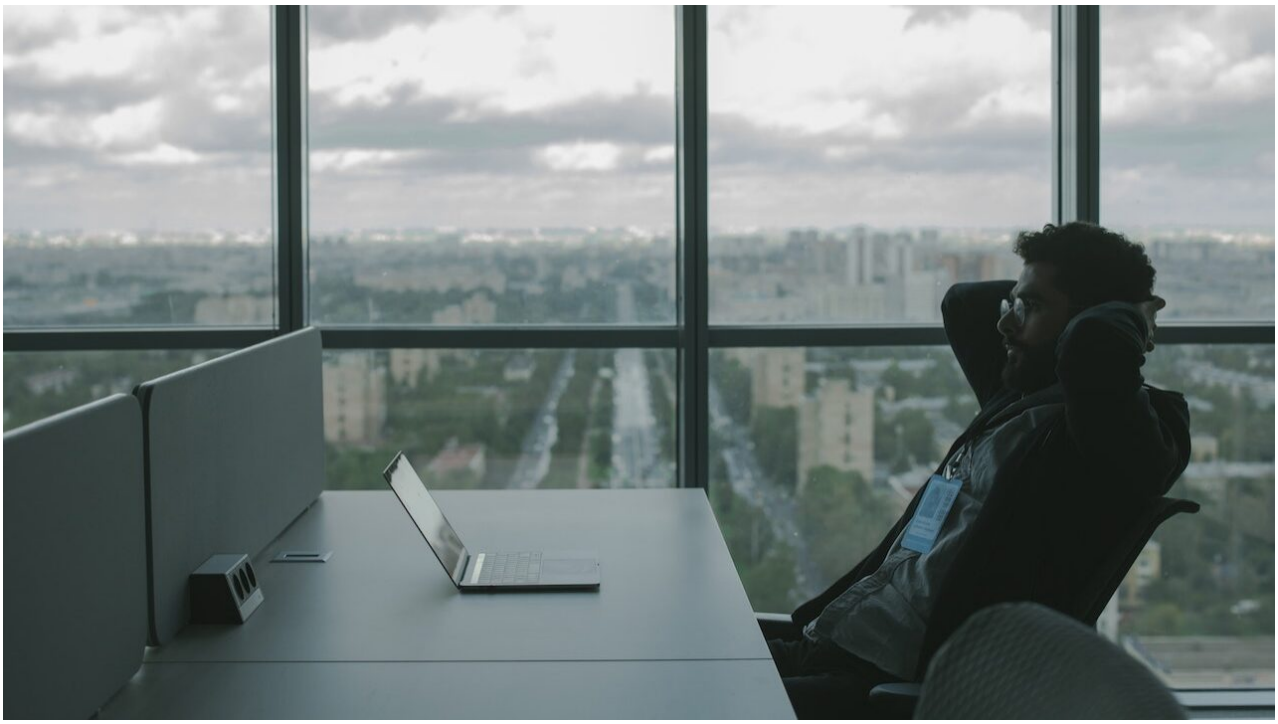
Em Espanha, no final de julho, alguns meios de comunicação – como o ABC, El Mundo ou Expansión – terão sido alvo de ataques por parte do grupo de *hackers* pró-Rússia, tendo os seus sites enfrentado vários problemas técnicos. Estes ataques, no entanto, surgiram já depois de outros ciberataques terem afetado várias páginas oficiais de diferentes entidades espanholas, como sucedeu com sites da família real espanhola, de diversos bancos ou do governo. O site do Ministério do Interior, inclusive, esteve inativo durante várias horas.

Embora a **tendência seja “crescente e exponencial para todo o mundo Ocidental”** – como avisa Bruno Castro – entre os os dias 19 e 26 de julho, a Visionware registou um total de 56 ataques em Espanha. E **as consequências para a “marca” Espanha são várias, sendo desde logo “gigantes” os danos reputacionais e a exposição mediática (negativa) dada ao país e às instituições espanholas com este acontecimento.**

2022 foi ano de ciberataques “de grande impacto”

“Por um lado, ficou patente perante todo o mundo, o alcance e o impacto causados pelos ciberataques de sucesso instaurados por este grupo cibercriminoso; por outro lado, deixou assim bem visível a enorme fragilidade e vulnerabilidade dos principais sistemas e infraestruturas digitais espanholas”, explica Bruno Castro.

Segundo o especialista, os ciberataques têm **custos elevados para a economia** (pela quebra, interrupção ou inatividade total dos negócios), ao mesmo tempo que **minam a confiança nos Estados** (naquela que é uma questão de imagem e de gestão da reputação).



Um ciberataque a uma PME pode mesmo levar à falência da empresa e à extinção de uma marca, alerta Bruno Castro.

**No caso das marcas, as implicações e consequências de um ataque deste género podem ser "devastadoras"**, principalmente quando se tratam de casos de *ransomware (software* malicioso que encripta os dados, indisponibilizando os sistemas, para posteriormente solicitar resgates financeiros) "altamente violentos" que "minam" todo o sistema. **Tratando-se o alvo, por exemplo, de uma PME (a grande fatia do tecido empresarial português), o ataque pode mesmo levar à falência da empresa e à extinção de uma marca.**

Contudo o impacto destes ciberataques vai além da própria empresa ou marca alvo do ataque. Segundo dados da Cybersecurity Venture, em 2021, **os ciberataques em todo o mundo custaram mais de cinco mil milhões de euros à economia mundial**, estimando-se ainda que este custo continue a subir 15% todos os anos até ultrapassar os **oito mil milhões de euros em 2025.**

Estes ataques informáticos "**têm custos elevados para economia e minam totalmente a confiança nos Estados, sendo que o seu impacto vai muito além das perdas económicas, com ciberataques recorrentes a infraestruturas críticas a corroerem a confiança dos cidadãos nos seus governantes**", aponta Bruno Castro.

Estes "danos" incluem a **destruição de dados**, a **perda de produtividade** das diferentes entidades afetadas, o **roubo de propriedade intelectual** e o **custo da reparação e/ou recuperação** total dos estragos gerados.

"**A própria imagem do país sai 'hackeada' ao revelar-se frágil, violável, delicada, gerando instabilidade política, económica, social, promovendo e fazendo o elogio do caos e da anarquia, tão desejados e procurados pelas ações levadas a cabo por este tipo de grupos criminosos**", afirma o especialista em cibersegurança.

## Em Portugal…

Mas não é só no país vizinho que decorrem estes ataques. Entre marcas presentes em Portugal, Bruno Castro destaca os ataques que tiveram maior impacto mediático no ano passado, em particular aqueles feitos ao grupo **Impresa** e o "super mediático ciberataque" à **Vodafone,** "algo inédito no nosso país, e que abriu um precedente em todo o setor IT e no próprio mundo (ou submundo) da área da atuação da cibersegurança".

"Nunca se falou tanto da importância e dos impactos da cibersegurança como até essa altura (e ainda hoje), e esse é um fator e uma consequência altamente positiva resultante de uma situação negativa e prejudicial para diversas empresas e inúmeros consumidores/particulares", afirma o especialista.


Para Bruno Castro, o ciberataque à Vodafone em Portugal resultou num "autêntico case study de sucesso (em termos de comunicação) no nosso país", ao contrário do ataque à TAP.EPA/DANIEL NAUPOLD

**Bruno Castro salienta e elogia o posicionamento e a comunicação veiculada por parte da marca de telecomunicações** que, num episódio inédito no país, optou por uma comunicação "clara e transparente" perante os clientes afetados, com conferências de imprensa e comunicados "quase em *real time*", a reconhecerem uma falha e a confirmação de um possível comprometimento de dados pessoais e confidenciais.

Vodafone diz que talvez nunca venha a saber razão do ataque

"**Um autêntico *case study* de sucesso (em termos de comunicação) no nosso país**", sumariza o especialista em cibersegurança e análise forense.

Já em sentido contrário, **a gestão dos ciberataques infligidos à TAP (que também ocorreram em 2022) "foi algo que deixou muito a desejar**, gerando os também já conhecidos impactos negativos na opinião pública e na imagem geral da nossa companhia de bandeira perante os seus clientes".

Ciberataque à TAP: o que disse a empresa (e o que aconteceu)

Esta visão negativa deriva de dois erros "crassos" na opinião de Bruno Castro, começando pela comunicação de que o ciberataque havia sido contido a tempo (sem comprometimento de serviço ou dados e informações) à qual se seguiu um desmentido – que já era um facto publicado no canal do grupo cibercriminoso – que veio revelar como "óbvia" a perceção da fuga e roubo de dados dos clientes da companhia aérea.

Num âmbito geral, segundo Bruno Castro, são "**vários os leaks que já aconteceram em Portugal associados à NATO e à defesa portuguesa**", também estes desencadeados por grupos pró-Kremlin, sendo prova disso os ataques registados a serviços estatais portugueses nos últimos meses. No entanto, Portugal tem feito "**imensos esforços a nível do Estado e a nível empresarial para aumentar a sua maturidade em termos de segurança cibernética**", nota o CEO da Visionware.

De acordo com os dados da quarta edição do "Relatório Cibersegurança em Portugal – Riscos & Conflitos", do Centro Nacional de Cibersegurança (CNCS), **as ciberameaças que mais afetaram o ciberespaço de interesse nacional em 2022** foram o "ransomware" a cibersabotagem/indisponibilidade, o "phishing" (emails fraudulentos) e "smishing" (SMS fraudulentos), a burla online e o roubo de credenciais e usurpação de identidades.

Entre as **principais vítimas de incidentes de cibersegurança encontram-se os setores da banca (sobretudo clientes), da educação e ciência, tecnologia e dos transportes, da saúde e da comunicação socia**l. O mesmo relatório revela ainda que, "**a perceção de risco de alguma entidade no ciberespaço de interesse nacional poder sofrer um incidente de cibersegurança aumentou em 2022 e 2023**", enquanto diminuiu "a perceção de que o ciberespaço está mais resiliente a ciberataques".

## O que fazer

Embora não exista nenhuma "fórmula mágica" para restringir estes ataques e o seu impacto nas empresas, marcas e pessoas, "**é necessário prevenir e investir em modelos de segurança contínuos, conhecer bem as infraestruturas, e sobretudo, 'stressar' constantemente os sistemas, procurando falhas e fragilidades, corrigindo-as de forma perseverante, de modo a 'blindar' a organização contra quaisquer eventuais tentativas de ataques**", refere Bruno Castro.

**A sensibilização e a maior "evangelização" sobre estes temas da cibersegurança** é também um fator de proteção adicional em matéria de segurança uma vez que, caso as pessoas evitem clicar em certos *links* e ignorem emails de endereços desconhecidos, podem evitar desta forma muitos riscos desnecessários e fugas de dados, ajudando a impedir um ataque bem-sucedido.

Dentro de um contexto empresarial, é também "fundamental" uma **crescente consciencialização e sensibilização dos colaboradores**, "devendo fazer parte da estratégia do programa de segurança de qualquer organização", desenvolvendo-se, por exemplo, ações de *phishing* simuladas.

A recolha de dados dos utilizadores por parte das marcas acarreta também perigos adicionais, contudo "**o incentivo para a recolha maximal de dados é demasiado grande (e vantajosa) para as empresas/marcas não o aproveitarem**", refere Bruno Castro, pelo que deixa o alerta de que "**um dos principais erros que as pessoas cometem quando utilizam uma aplicação é presumir que esta, simplesmente por estar disponível, é completamente segura**".