Internet. Haverá "bombas-relógio" para prejudicar políticos em Portugal?

A campanha eleitoral para as legislativas vai arrancar. A atividade dos partidos e dos políticos intensifica-se. Será que estão todos conscientes dos riscos que correm na rede? Há quem diga que não.

PAULA SÁ

Um político da nossa praça recebeu um conjunto massivo de *e-mails* com conteúdo de interesses pessoal. Perante a insistência, acabou por abrir um "nocivo" e os seus dispositivos foram infetados com *software* malicioso, o que permitiu ao "atacante" monitorizá-lo, em tempo real, sem que se apercebesse. Foram roubadas *passwords*, os *e-mails* devassados e marcados todos os *sites* visitados. O perfil tinha sido traçado para conseguir cativar a atenção do político em causa e com um fim muito preciso: utilizar a informação como "bomba-relógio" no decorrer da campanha eleitoral para o prejudicar.

Este caso é relatado, sem a identificação da vítima, por Bruno Castro, sócio da VisionWare, uma empresa de segurança informática, credenciada pelo Gabinete Nacional de Segurança, que tem contratos com as principais câmaras do país e com muitas das instituições do Estado, incluindo a Procuradoria-Geral da República há dez anos.

"Os partidos e os políticos estão muito expostos e não estão atentos à cibersegurança e a vulnerabilidade aumenta em períodos eleitorais", afirma o especialista. Bruno Castro lembra que, até por questões geracionais, numa comunidade política em que muitos dos seus agentes vieram de uma época pré-digital, há ainda muito desconhecimento do que de nocivo pode acontecer.

A VisionWare trabalha com a distribuição, empresas como a Galp e a banca e no meio político, onde chegou mais tarde. E porquê esta aposta tardia na cibersegurança vocacionada para os políticos? "É o setor mais complexo", garante Bruno Castro. A explicação é simples, enquanto nas empresas se pode "trabalhar a jusante", prevenindo os perigos, nos partidos políticos e nos políticos a comunicação é mais aberta e imediata com os militantes e eleitores.

Além disso, muita da comunicação política, sobretudo, em períodos de campanha eleitoral, já é muito feito através das redes sociais.

"Os ataques são mais recorrentes do que se pensa", afirma Bruno Castro. Diz que há um conjunto de grupos que oferecem serviços de "pirataria informática" para obter informações sobre o político A e B. Há também muita informação que facilmente é truncada e que depois se torna viral.

"No meio de uma conversa de rede social posso alterar parte do conteúdo e estancar depois o fluxo é quase impossível." O especialista em cibersegurança frisa que "é incalculável o dano que uma mensagem maliciosa numa conta oficial de um partido pode causar até ser retirada ou desmentida. A experiência mostra que o desmentido nunca é tão viral como a mensagem provocatória".

Mas há também o risco, diz, de ocorrer em Portugal o que se passou nas eleições presidenciais americanas de 2016, em que houve manipulação da opinião pública através das redes sociais, com recurso a *trolls*, ou seja perfis *online*, muitas vezes falsos, que deliberadamente manipulam outros internautas, empolando discussões ou fazendo circular a informação falsa, as *fake news*.

Aliás, as eleições para a Casa Branca em 2016 foram profícuas nos ataques cibernéticos. Foi através de um *e-mail* da Google, aparentemente legítimo, que John Podesta (em março de 2016), responsável pela campanha de Hillary Clinton, ficou com o *e-mail* infetado, o que permitiu o acesso à sua conta e, meses mais tarde (outubro de 2016), a divulgação de milhares de *e-mails* pessoais no *site* WikiLeaks.

> "Mesmo que auditássemos um sistema desses [o voto eletrónico] mil vezes não conseguiríamos passar um cheque em branco."

"Temos de ir despertando os políticos para não fazerem no mundo digital o mesmo que não fazem no mundo físico, como falar com estranhos sem ter cuidado. Mas no sofá há uma sensação de segurança diferente", diz Bruno Castro e admite: "No que diz respeito à cibersegurança dos políticos é uma guerra que ainda estamos a perder. Porque temos uma ação que é a de tentar impedir cem balas ao mesmo tempo."

E é precisamente porque considera que os sistemas não são 100% invioláveis, que não é favorável ao voto eletrónico. "Mesmo que auditássemos um sistema desses mil vezes não conseguiríamos assinar um cheque em branco. E a possibilidade de furar um sistema destes seria catastrófico para a democracia", sublinha o especialista em cibersegurança.

Nível de sofisticação baixo

O deputado socialista e membro do Conselho Nacional de Cibersegurança José Magalhães garante que, apesar de tudo, não se têm verificado "casos espetaculares" de ataques na internet a políticos ou partidos em Portugal. Tem uma explicação prosaica para este facto: o "nível de sofisticação" dos partidos no ciberespaço a nível nacional ainda é muito fraco e não gera o apetite dos *hackers*.

José Magalhães afirma que a União Europeia já se preparou para os ciberataques ao instituir uma rede rápida de alerta que funcionou nas eleições, em que cada Estado membro daria nota caso se registasse alguma situação irregular. "A rede de alerta rápido não registou ocorrências significativas e não houve nenhum episódio que justificasse medidas de emergência", diz o membro do Conselho Nacional de Cibersegurança.

O Centro Nacional de Cibersegurança (CNCS) tem feito ações de sensibilização junto de deputados, o que acontecerá também nestas eleições, a par de um gabinete de acompanhamento para o dia das legislativas. O CNCS também fará este tipo de ações junto dos responsáveis pelas campanhas dos vários partidos e ações de sensibilização nas redes sociais destinadas aos cidadãos com particular enfoque na desinformação.

O diretor-geral do CNCS, almirante António Gameiro Marques, lembra ao DN que por ocasião das eleições europeias o centro fez um exercício em abril subordinado ao tema, que tem vindo a preocupar as autoridades. "Já tínhamos a perceção do problema, até por comparação com o que se passou a este nível em países como Estados Unidos, Reino Unido, França e Catalunha." E frisa que a própria UE, que nos próximos quatro ou cinco anos vai ter muitos atos eleitorais, pediu aos Estados membros que tomem medidas para impedir ciberataques. O almirante, que desempenha o cargo de diretor-geral do CNCS há três anos diz que a sensibilização da comunidade política para os perigos da internet têm vindo a crescer. "É um tema que está cada vez mais na ordem do dia, com impactos políticos e estratégicos a nível mundial", diz, mas lembra que a segurança neste campo "é um trabalho persistente e perseverante, que faz parte da evolução e da maturidade da sociedade atual".