AUTÁRQUICAS

Detetar 'fake news' eleitorais já é oportunidade de negócio

Empresa portuguesa Visionware junta recursos informáticos e humanos para detetar ataques contra os candidatos que são seus clientes e repor a verdade. Algo que significa a "verdade do cliente", tirando nos casos mais graves.

ANTÓNIO FREITAS DE SOUSA
afsousa@jornaleconomico.pt

Cristina Bernardo

Os ataques informáticos são cada vez mais uma constante de todos os dias e, como não podia deixar de ser, as eleições (no caso, as autárquicas) "constituem um pico" de atividade ilegal, com a multiplicação de veículos de disseminação de notícias falsas que visam "partidos, candidatos e tudo o que envolve as campanhas", num cenário em que a simples observação empírica da realidade das redes sociais já não é suficiente para a sua deteção.

Bruno Castro, CEO da Visionware, líder do mercado na área da segurança informática, tem nestas alturas trabalho reforçado. "A pandemia trouxe para a Internet tudo o que ainda não estava lá", explica, ciente de que a rede global passou a ser "o ponto de encontro" de tudo e de todos. "Nos últimos 18 meses, a atividade em termos de notícias falsas aumentou muito", e por definição o momento eleitoral é especialmente delicado. Sem poder revelar a identidade dos seus clientes nesta área, afirma que já é praticamente impossível, a qualquer candidato ou candidatura, gerir este tipo específico de ataque.

A máquina antes do homem

"A nossa principal função é identificar o mais rapidamente possível um ataque informático que pretenda lançar notícias falsas sobre um cliente e contra-atacar antes que essa notícia passe a ser viral", diz o CEO da Visionware, pois a partir desse momento "já não há nada a fazer".

Como não poderia deixar de ser, são as máquinas que estão encarregadas de detetarem o início de um ataque. "Montamos uma espécie de 'big brother' que, através de palavras-chave e da análise de um conjunto de veículos, detetam a possibilidade de um ataque por via de notícias falsas", explica. Só depois disso entra em ação o génio humano – que substitui a máquina para perceber a extensão do ataque e escolher uma forma de contra-ataque. "É uma segunda triagem, desta vez feita pelos colaboradores da empresa" – que de seguida ligam ao cliente para perceberem se há de facto uma mentira a iniciar circulação, e que verdade deve ser reposta em sua substituição.

Há que referir que, nestes casos onde não se configura um crime de proporções graves, a verdade do cliente é suficiente: se essa verdade também for uma mentira, isso é da responsabilidade do contratante. Só nos casos em que a empresa considera a necessidade de alertar as forças da ordem é que as coisas deixam de ser simples e obrigam a uma verdadeira investigação.

Uma investigação aprofundada da origem das notícias falsas que bombardeiam a classe política dificilmente chegaria a qualquer conclusão: qualquer iniciado na gestão da Internet consegue facilmente "apagar os indícios da sua passagem pelas redes sociais", fazendo encalhar qualquer tipo básico de análise. "É muito difícil identificar a pessoa por trás da disseminação de notícias falsas", refere Bruno Castro – até porque um perfil falso aberto nas redes sociais pode desaparecer rapidamente sem deixar rasto e ser substituído por outro que continuará a fazer o 'serviço'. "É o que acontece constantemente", refere o CEO da empresa.

O tipo de serviço prestado pela Visionware está longe – cada vez mais longe – de ser mero paliativo: "A forma como as redes sociais estão construídas propicia" a existência deste tipo de incidentes e tudo indica que nada vai ser alterado num futuro próximo. Pelo contrário, "a exposição às redes será cada vez maior", assim como será cada vez maior a facilidade com que a vida de cada um pode ser vasculhada através da Internet.

Bruno Castro
CEO da Visionware

Só nos casos em que a empresa considera que existe necessidade de alertar as forças da ordem é que as coisas obrigam a uma verdadeira investigação

Bom-senso s.f.f.

"Como é que nos defendemos disso? Com bom-senso. E adaptando a forma como nos movemos na vida real à forma como nos movemos nas redes. Nunca falar com estranhos, nunca andar por caminhos escuros". É isso que se faz na vida real e na vida virtual dentro do Internet, afirma Bruno Castro.

O currículo de alguém como o CEO da Visionware é também uma experiência diferente: não está cheio de mestrados e doutoramentos (tê-los-á por certo), mas de notações que remetem para os policiais: licenciado em Engenharia Eletrotécnica pela Faculdade de Ciências e Tecnologia da Universidade de Coimbra, onde obteve o grau de mestre em Engenharia Informática (Segurança Informática), está credenciado NATO-Secret e Nacional Secreto, faz parte do grupo de auditores de segurança credenciado pelo Gabinete Nacional de Segurança, é *lead auditor* e *lead implementer* na norma ISO/IEC27001, BS25999 atribuídas pela British Standards Institute (BSI), CIPP/E Certification - Privacy's Premier European Data Protection Certification e CIPM Certification - Certified Information Privacy Manager.

A Visionware é uma empresa portuguesa criada em 2004, tem atualmente cerca de 60 colaboradores em escritórios em Lisboa e Porto e é especializada em segurança da informação – cibersegurança, TI, investigação forense, *compliance*, privacidade, formação e *intelligence*. Desenvolve projetos de elevada complexidade e trabalha com clientes dos sectores público e privado, em áreas como indústria, saúde, banca e finanças, telecomunicações, governo e defesa, e autoridade pública. Com cerca de três milhões de euros de volume de negócios – divididos em partes iguais entre projetos nacionais e no estrangeiro – a empresa tem os seus clientes espalhados por todo o mundo, incluindo o Médio Oriente, a África "e também, por exemplo, a Comissão Europeia". ■