CRÓNICA DO OBEGEF
Nº 61 /2023-03-30
http://www.obegef.pt

Miguel Morais Abrantes

> > Encriptação Incompleta

A confidencialidade e a integralidade da informação armazenada em bases de dados e transmitida através meios eletrónicos é essencial para o funcionamento de organizações, públicas e privadas, mas também para preservar o património e a vida privada dos cidadãos.

Assim, a crescente utilização de meios eletrónicos para armazenar e transmitir informação foi acompanhada, embora com atraso, por medidas destinadas a salvaguardar a sua confidencialidade e integralidade.

De entre as referidas medidas assume predominância a encriptação, a qual consiste na utilização de *software* destinado à transformação de dados através de um algoritmo que inviabiliza a sua leitura. Para ter acesso aos dados encriptados é necessário dispor de uma chave de desencriptação, que apenas é fornecida aos destinatários da informação.

O *software* de encriptação é utilizado por quem pretende proteger dados: entidades públicas, empresas privadas e cidadãos, mas também por países hostis e organizações criminosas.

Segundo informação prestada por Edward *Snowden* (um antigo analista de sistemas da NSA - *National Security Agency*), desde 2009 a NSA gastou mais de 800 milhões de dólares na materialização do «SIGINT», um programa que «envolve ativamente indústrias de tecnologias de informação estrangeiras e americanas para influenciar e/ou explorar abertamente o *design* de produtos comerciais».

Segundo o mesmo antigo funcionário da NSA, para a referida agência de informações, o desenvolvimento da sua capacidade para ultrapassar a encriptação é essencial para conseguir controlar o terrorismo internacional. Todavia, a atividade secreta que a NSA está a desenvolver pode ter consequências negativas.

Pois, a forma como NSA quer atingir os seus objetivos, ainda segundo Edward *Snowden*, traduz-se em inserir falhas nos sistemas de encriptação. Desta forma, a NSA torna estes sistemas exploráveis, não só por agências governamentais, mas também por todos os que consigam explorar as lacunas introduzidas em dados ou comunicações encriptados.

Conforme, já foi várias vezes referido, «Paradoxalmente, ao tentar tornar a América mais segura, a NSA tornou as comunicações americanas menos seguras. Minou a segurança de toda a Internet».

Todavia, não foram apenas as comunicações americanas que ficaram menos seguras. Pois, num mundo globalizado, quando se introduzem lacunas em sistemas de informação de empresas multinacionais, também se tornam menos seguros sistemas de informação que geram dados sensíveis em todo o mundo.

Cientes da ameaça que a vulnerabilidade dos seus dados representa, empresas gestoras de infraestruturas essenciais (através das quais se processa o fornecimento de água, eletricidade, gás ou comunicações) gastam elevadas quantias para incrementar a segurança.

Porém, quando agências de informações, para salvaguardar a segurança interna, introduzem lacunas em sistemas que gerem essas infraestruturas, não são apenas elas que adquirem a possibilidade de controlar os sistemas, são também as agências de informação de países hostis e piratas informáticos que ficam com a porta aberta para violar a encriptação necessária para que a vida dos cidadãos funcione com normalidade.