CRÓNICA VISÃO ELECTRÓNICA
Nº 406 / 2016-10-27
http://www.gestaodefraude.eu
Edgar Pimenta

>> As duas faces de uma mesma moeda!

Somos, cada um de nós, geradores de cada vez mais informação. A nossa pégada digital é cada vez maior e nem sempre (ou raramente) está no nosso controlo. Talvez também por isso, existe cada vez mais regulamentação de como deve ser tratada a informação gerada por cada um de nós. Um exemplo é o mais recente Regulamento Geral de Proteção de Dados Pessoais.

E seja por necessidades regulamentares/legais ou por mera preocupação, a verdade é que, cada vez mais, existe a necessidade de proteger toda essa informação.

Esta proteção pode ser alcançada de várias formas e a vários níveis mas o seu objetivo é só um - assegurar a segurança da informação. Relembrando e de forma sucinta, a segurança da informação tem 3 vertentes:

- Confidencialidade - garantir que a informação apenas está acessível a quem dela realmente necessita;
- Integridade - a informação deve ser fidedigna e real, sem erros nem omissões;
- Disponibilidade - sermos capazes de aceder à informação quando dela necessitamos.

focando-nos na confidencialidade.

Existem várias formas de proteger a confidencialidade da informação. Uma das mais utilizadas é a encriptação, atualmente efetuada com base em algoritmos matemáticos relativamente complexos mas que são, muitas vezes, publicamente conhecidos. E são conhecidos porque a robustez da encriptação suporta-se no algoritmo mas baseia-se sobretudo na chave secreta que é usada.

Muitos destes algoritmos são suportados por elevadas capacidades de processamento. Mas não foi sempre assim.

A encriptação não é uma tecnologia do século XXI. Nem sequer do século XX. Acredita-se que o exemplo de algoritmo de encriptação mais antigo terá mais de 2000 mil anos (não, não foi um

CRÓNICA VISÃO ELECTRÓNICA
Nº 406 / 2016-10-27
http://www.gestaodefraude.eu
Edgar Pimenta

lapso de escrita).

Já os gregos antigos e os espartanos usavam o Scytale para comunicar remotamente de forma secreta. O algoritmo é muito simples: um pergaminho era enrolado à volta de um prisma hexagonal ("cilindro" com 6 faces) onde era escrita a mensagem. O mensageiro transportava depois o papiro, ciente de que se alguém o apanhasse não seria capaz de perceber a mensagem. Isto porque para ler a mensagem era preciso voltar a enrolar o papiro num prisma semelhante aquele onde a mensagem tinha sido escrita (e que o mensageiro, obviamente, não transportava). Simples e engenhoso.

Ainda hoje, a encriptação é uma forma muito eficaz de proteger a informação. Seja quando ela está "parada", residente nos nossos sistemas, seja quando circula pela internet.

Mas se serve para proteger a nossa informação, também está protegida a transmissão de informação de pessoas mal intencionadas (ex. terroristas). E esse é um dos reversos da medalha da encriptação (e um pouco de toda a segurança da informação). O que nos protege também nos pode expor. Não diretamente, mas porque aqueles que nos devem proteger ficam também condicionados por estas ferramentas. Claro que foram já vários os governos que tentaram ter formas de desencriptar a informação sem a devida autorização dos autores das mensagens. Mas se tal deve ou não ser feito é uma longa discussão. Uma discussão sensível entre a privacidade, a liberdade e a segurança (no sentido físico do termo).

Recentemente, a encriptação começou a ser mais falada por outros motivos: o *ransonware*.

Este tipo de *malware* faz algo simples quando ataca: procura informação no equipamento do utilizador e cifra essa mesma informação. E apenas após o pagamento de um resgate é fornecida a chave que permite recuperar a informação. Mais uma vez, simples mas eficaz. Precisamente por isso apresenta um crescimento tremendo: estima-se que em 2015 foram pagos cerca de 22 milhões de euros e que este ano poderão atingir os 1000 milhões.

Existem algumas medidas de proteção, sendo que algumas são as típicas contra todo o tipo *malware*:

CRÓNICA VISÃO ELECTRÓNICA
Nº 406 / 2016-10-27
http://www.gestaodefraude.eu
Edgar Pimenta

1. um bom antivírus atualizado;
2. não carregar em links nem abrir ficheiros de origens desconhecidas;
3. não andar em sites duvidosos.

Contra o perigo do *ransomware*, efetuar backups periódicos e telos devidamente salvaguardados é fundamental. Fundamental também, e muitas vezes menosprezado (infelizmente), devem avisar a polícia. Para vários tipos de *ransomware* existem já chaves e processos de recuperação e a polícia poderá ajudar. E a própria polícia necessita dessa informação para que esteja mais capacitada para atuar. E já agora…. Alguns *ransomware* nem sequer cifram os dados - é um resgate falso.

Um pequeno exemplo de como na segurança, uma mesma moeda tem várias faces. E a sua resolução é tudo menos simples. Porque o mundo ciber é vasto, complexo e ainda está a dar os primeiros passos.