Edgar Pimenta

> > Segurança ou outros pretextos?

Quem anda nos meios de Segurança de Informação desde o século passado sabe que nos anos mais recente este tema tem ganho uma relevância cada vez maior, deixando de ser um tema esotérico que é preocupação de "meia-dúzia" de pessoas estranhas, para passar a ser um tema discutidos por muitos.

Essa evolução resultará de vários fatores que para isso contribuíram:

- Privacidade – As questões da privacidade ganharam dimensão nos últimos anos, sem dúvida alavancados pelas regulações de privacidade e nomeadamente pelo Regulamento Geral de Proteção de Dados (RGPD). Isto porque se existem muitas componentes do RGPD que são processuais, a verdade é que, no limite, os dados pessoais devem ser mantidos seguros.

- Dinheiro digital– Nada nos preocupa mais do que nos irem ao bolso. É uma verdade de *La Palisse*. Paralelamente, nos últimos anos o dinheiro vem-se tornando mais digital. Seja pela facilidade com que lhe acedemos (*homebanking*, aplicações para o telemóvel, etc..) seja pelo emergir das novas moedas digital como a *Bitcoin* ou a *Ethereum*. No primeiro caso, se se torna mais fácil para nós aceder e transacionar o nosso dinheiro, também por vezes se torna mais fácil que outros o façam (obviamente, de forma indevida). E a necessidade de melhorar a usabilidade tentando manter a segurança implica que esta última seja considerada de uma forma mais séria. Por outro lado, o uso de moedas digitais não rastreáveis (as tais Bitcoins...) veio aumentar o uso destas em ataques como os do *ransomware*. E o facto destes ataques terem impactos significativos nas empresas, faz que com estas olhem seriamente para a necessidade de proteger os seus ativos.

- (wiki/NSA/SLB) *leaks* – Estes e outras fugas de informação vieram dar visibilidade ao impacto que a falta de proteção da informação pode originar (se duvidas havia).

Havendo com certeza muitos outros fatores, estes parecem ser bastante relevantes.

Recentemente, assistimos a um novo fenómeno: a segurança como arma de arremesso comercial/diplomática. Estou a referir-me especificamente ao caso Huawei e aos Estados Unidos.

Se uma empresa ou um Estado quiserem deixar de usar uma empresa ou serviço por questões de segurança, devem fazê-lo. Aliás... deve ser um critério de avaliação para a utilização de novos fornecedores (e validação dos atuais): como estes endereçam a segurança. Como tal, o princípio em causa faz todo sentido. Mas neste caso específico, não deixa de ter algumas ironias, nomeadamente o facto dos Estados Unidos, durante vários anos, terem usado ferramentas diversas (incluindo equipamentos fornecidos por empresas americanas) para espionar diversos Estados em várias localiza-

ções. Ou mais do que uma ironia, existirá um conhecimento de que esse tipo de "espionagem" é de facto bastante produtiva e por isso perigosa quando o feitiço se vira contra o feiticeiro?

Por outro lado, é fácil acreditar que o Estado chinês poderia ter a tentação de usar os seus fabricantes de tecnologia para conseguir espiar outros Estados. Já várias notícias foram divulgadas que apontam nesse sentido mas sem factos que as sustentem de forma definitiva.

Mas falta uma peça neste puzzle... Ou os Estados Unidos possuem alguma informação concreta relacionada com a insegurança dos equipamentos da Huawei e não a estão a divulgar ainda que de forma restrita (acreditando que a ordem executiva a proibir o uso da Huawei não foi apenas por questões económicas) ou a Europa é muito *naive* e incapaz de fazer uma avaliação adequada sobre a segurança do equipamento desse fornecedor (e aí seria um atestado de incompetência).

A bem da segurança, seria fundamental perceber exatamente a peça do puzzle que está em falta. Só assim poderemos efetivamente melhorar o estado da nossa (in)segurança.