Cibersegurança, Intelligence e Cisnes Negros

dinheirovivo.pt/opiniao/ciberseguranca-intelligence-e-cisnes-negros-14365570.html

Recentemente, foi referido na imprensa que a Áustria estava a preparar a sua população, com recomendações e exercícios públicos, para um risco crescente de interrupção no abastecimento de eletricidade.

Quando questionados sobre o assunto, tanto o Gabinete Nacional de Segurança como o Centro Nacional de Cibersegurança de Portugal excluíram a necessidade de levantar preocupações idênticas no nosso país, não deixando, contudo, de referir que há um histórico real para este cenário, muitas vezes provocado por ciberataque.

A menos de dois meses do final do ano, numa altura em que, um pouco por todo o mundo, se volta a discutir a possibilidade de regressar a um cenário de confinamento parece-me fundamental fazer-se um "Shift" na forma como interpretamos e levamos a sério o que se passa no mundo. Neste sentido, há duas dimensões que quero abordar e que estão intimamente ligadas.

Conhecer os acontecimentos locais, nas suas vertentes económica, política e social, e compreender o seu impacto potencialmente global não é só uma questão de gosto ou de interesse intelectual. Esse conhecimento permite-nos antecipar decisões, identificar tendências, evitar erros e aplicar melhor soluções, seja num negócio, seja num governo de um país. Esta que é apenas uma parte daquilo que serviços de intelligence públicos e privados fazem, é uma das mais antigas formas de reduzir o risco e também de detetar oportunidades e hoje, num contexto em que a informação circula também no ciberespaço, ganha renovada importância.

Ora, nós, indivíduos, organizações e mesmo governos, também circulamos no ciberespaço. As nossas estruturas estão, na sua maioria, conectadas. Não somos apenas recetores da informação que aí circula e das vantagens que a conectividade representa. Ao existirmos ativamente nesta nova realidade paralela, também deixamos uma pegada digital e sujeitamo-nos a um conjunto de novos riscos e interconexões com outros indivíduos ou organizações que, de uma forma "lúcida", desconhecíamos que poderiam existir. Assim, sem as devidas proteções, o simples facto de existirmos no ciberespaço pode ser o suficiente para deixarmos a descoberto informações sensíveis ou darmos acesso indevidamente ao controlo da nossa atividade digital, seja ela de cariz profissional ou profissional. É aqui que entra a importância da cibersegurança.

Falar em ciberataques capazes de provocar apagões elétricos não é matéria futurista.

Mesmo considerando baixa a possibilidade de sermos alvos de um ataque coordenado à infraestrutura elétrica do país, não me parece que as Instituições públicas responsáveis pela componente de "homeland security" digital de Portugal, tenham querido, intencionalmente, desvalorizar o exercício a que a Áustria se propõe ou o risco de ciberataque às infraestruturas críticas deste ou de qualquer outro país. Isto porque, no

domínio da segurança, nunca se está suficientemente bem preparado. O risco mitiga-se pela persistência. É preciso testar com frequência a estrutura, e testá-la para diversos cenários, inclusive os menos prováveis, pois é para esses que estaremos sempre menos preparados.

Isto recorda-me a teoria do cisne negro, que se refere a acontecimentos tão improváveis quanto disruptivos. Ao longo destes dois anos falou-se várias vezes que a pandemia de COVID-19 poderia tratar-se de um exemplo desses, mas a verdade é que o risco de pandemia não era improvável.

Não estou a dizer com isto que nos devemos preparar imediatamente para a inevitabilidade de um apagão elétrico, mas creio ser urgente pôr em prática as ferramentas que já temos, como é o caso da cibersegurança, para avaliar continuamente o nosso nível de segurança, e por inerência, proteger as estruturas críticas (entre outras) que suportam o País, e a vertente de intelligence, para antecipar as ameaças, tal como os nossos pares já se estão a preparar para tal.

Bruno Castro, CEO da Visionware