OPINIÃO

ARNALDO COSTEIRA
DIRETOR-GERAL DE COMUNICAÇÃO E RELAÇÕES EXTERNAS DO ISEC LISBOA
DOCENTE UNIVERSITÁRIO

CASA ARROMBADA...

A cada minuto que passa são gerados, em todo o mundo, mais de 1,5 mil terabytes de dados, um verdadeiro tsunami de informação que se agiganta à razão de mais de 40 trilhões de gigabytes de dados por ano. Grande parte dessa informação é sobre nós! São os nossos dados pessoais, informação classificada e sensível sobre os nossos comportamentos e consumos, são as nossas empresas e instituições virtualizadas a que acedem mais de 6 bilhões de dispositivos (smartphones e computadores).

Falar em segurança da informação é considerar esta área de exposição praticamente ilimitada, em que o risco à privacidade dos nossos dados é tanto maior quanto maior é o número de dispositivos que usamos no acesso a informação sensível.
Há uma ideia errada de que a cibersegurança é problema exclusivo das empresas, mas temos que ter consciência de que todos contribuímos a cada instante, com os nossos dados pessoais, hábitos e interesses, partilhados em plataformas de compras, entretenimento, informação e ensino.
O RGPD trouxe enormes desafios às organizações na garantia da privacidade dos dados pessoais, mas a dependência crescente das redes sociais, do armazenamento de dados na cloud e do recurso a SaaS e a servidores remotos, trouxe-nos a um patamar em que o controlo da informação já não está na dependência do seu titular.
A pandemia ampliou o risco, pela iliteracia digital e pelo aumento de acessos remotos à informação empresarial.
O objetivo deste artigo de opinião é o de trazer uma reflexão sobre os níveis de alerta e atenção que devemos ter, enquanto decisores nas nossas instituições, para os sistemas de segurança e controlo no acesso à informação que produzimos e dos dados pessoais com que estamos comprometidos em garantir a privacidade.
Organismos como o CNCS, que lidera o esforço de sensibilização dos cidadãos e das empresas para as boas práticas no acesso e gestão da informação e de comportamentos a adotar enquanto utilizadores da Internet, abrem caminho à literacia digital redutora das ameaças do cibercrime, mas cabe-nos a nós, todos, o dever de buscar o conhecimento e desenvolver competências que nos permitam adotar comportamentos e sistemas de controlo e segurança, para estarmos melhor preparados para as ameaças e ataques cada vez mais sofisticados.
Casos como o da Vodafone ao nível da cibersegurança, ou da Câmara Municipal de Lisboa ao nível da proteção de dados, são exemplos de que o risco e a falha são uma questão de tempo.
Não podemos continuar na expectativa de 'se' pode acontecer, mas na certeza de que, sendo uma inevitabilidade, devemos estar preparados para 'quando' acontecer.
A formação e a capacitação de todos quantos têm em mãos a gestão de dados e da segurança de informação é fundamental a este esforço coletivo que temos que fazer, em linha com a estratégia nacional de cibersegurança e da proteção de dados. A nós no CESICP, e no ISEC Lisboa enquanto instituição de ensino superior, compete-nos fazer a nossa parte, disponibilizando as ferramentas e conhecimentos potenciadores deste saber-fazer. E é o que fazemos.