RICARDO HENRIQUES

OPINIÃO

Ciberataques: preparado para o próximo?

Neste mundo em que a tecnologia está cada vez mais presente e a consciencialização da necessidade de um elevado grau de segurança por parte dos utilizadores é ainda baixa, a questão já não é "se" os ciberataques vão ocorrer, mas "quando" vão ocorrer.

2 de Dezembro de 2016, 12:59

Com milhões de pessoas ligadas à rede e a Internet das Coisas a multiplicar o número de dispositivos conectados de forma exponencial, prevê-se uma transformação do mundo digital que conhecemos, marcada pelo aumento da utilização da computação em nuvem e de dispositivos inteligentes com sensores que recolhem, tratam e comunicam dados, incluindo dados pessoais, de uma forma constante.

Esta realidade traz consigo um aumento do risco da segurança da informação, em especial da cibersegurança, do furto de informações pessoais, dados sensíveis, propriedade intelectual e segredos de negócio. Torna-se, por isso, necessária uma melhoria da segurança dos sistemas utilizados para essas comunicações.

Os incidentes de segurança são cada vez mais complexos e os prejuízos podem ser significativos. Basta pensarmos nas notícias de casos de "ransomware" (em que o atacante encripta os arquivos da vítima e informa-a que os documentos só serão recuperados se pagar o "resgate") ou de ataques a infraestruturas essenciais (tais como: comunicações, cuidados de saúde, socorro e emergência, água, energia, transportes) e o impacto que podem ter. Apenas uma pequena parte das empresas está preparada para estas situações.

A Estratégia de Cibersegurança da Comissão Europeia, definida desde 2013, levou a um volume significativo de nova legislação europeia relacionada com a cibersegurança, a qual culminou agora com a sua "pedra angular", a Diretiva de Segurança das Redes e da Informação (SRI), que tem como principal objetivo unificar as abordagens fragmentadas para a SRI que existe atualmente em toda a União Europeia (UE). A Diretiva foi adotada em 6 de julho de 2016, tendo os Estados-Membros da UE até 10 de maio de 2018 para transpor esta legislação para o direito interno.

Esta Diretiva estabelece obrigações de cibersegurança para os operadores de serviços essenciais (energia, transportes, banca, mercados financeiros, saúde, abastecimento de água e de distribuição e infraestrutura digital) e prestadores de serviços digitais (plataformas de comércio eletrónico, portais de pagamento pela Internet, redes sociais, motores de pesquisa, serviços de computação em nuvem ou lojas de aplicações online), mas as duas categorias ficam sujeitas a regimes diferentes. Para muitas entidades, esta Diretiva impõe pela primeira vez uma obrigação de comunicação de incidentes de segurança.

Um outro diploma que importa também salientar é o Regulamento Geral de Proteção de Dados (RGPD) que representa uma grande revisão das leis europeias de proteção de dados existentes. O RGPD foi adotado em 27 de abril de 2016. Ao contrário da diretiva SRI, este é um regulamento e, portanto, diretamente aplicável nos Estados-Membros. No entanto, há um período de transição de cerca de dois anos, tendo as organizações até 25 de maio de 2018 para colocar as suas práticas em conformidade com as novas regras.

Os responsáveis pelo tratamento de dados pessoais terão de adotar as medidas técnicas e organizativas adequadas para proteger os dados pessoais que tratam, devendo impor a mesma obrigação nos seus contratos com prestadores de serviços, que passam agora também a ser responsabilizados diretamente no RGPD. Também o RGPD introduz obrigações de notificação às autoridades, no caso de violações de segurança no tratamento de dados.

Neste mundo em que a tecnologia está cada vez mais presente e a consciencialização da necessidade de um elevado grau de segurança por parte dos utilizadores é ainda baixa, a questão já não é “se” os ciberataques vão ocorrer, mas "quando" vão ocorrer.

Falhas em qualquer área de segurança podem resultar em pesadas multas e outras sanções contra a empresa. Além disso, a incapacidade de proteger a informação privada ou confidencial pode levar a ações judiciais por negligência, divulgação não autorizada de dados pessoais ou violação de obrigações contratuais de proteção da confidencialidade para clientes ou parceiros comerciais. A criação de uma estratégia para combater ciberataques é fundamental e implica o mapeamento e análise de todo o sistema, identificando como e por que motivo os dados são armazenados, bem como testes para identificar possíveis vulnerabilidades. Para tal é necessário ter meios e pessoal para lidar com estes temas de um ponto de vista técnico, legal e de relações públicas, de uma forma rápida e eficiente.

A segurança é geralmente percecionada pelas empresas como um custo obrigatório, uma despesa a pagar para estar em conformidade com a lei. É necessário mudar esta perspetiva para um modelo em que a segurança seja percecionada como uma mais-valia, não só de gestão de risco e minimização de danos, mas também para ganhar a confiança dos clientes na utilização da tecnologia.