



BRANDS' ADVOCATUS

Proteção jurídica de ataques cibernéticos

Por CRISTINA ROGADO

Advogada da CMS
Rui Pena & Arnaut

Os riscos cibernéticos são uma ameaça real para as empresas

Um estudo da consultora Marsh, de 2016, concluiu que 25% das empresas inquiridas em Portugal tinham sido vítimas de ataques cibernéticos nos últimos 12 meses e 38% das empresas envolvidas no estudo identificavam o risco cibernético como o seu principal risco corporativo. Efetivamente, as empresas hoje dependem das suas bases de dados pessoais e corporativos que são essenciais – senão vitais – para o desenvolvimento da sua atividade e qualquer organização que armazena dados está sujeita a este risco. Que riscos são estes? Estamos a falar de ataques de 'hackers', possibilidade de divulgação pública de dados, falhas de segurança do sistema, contaminação da base de dados com vírus, entre outros. E estes riscos podem resultar em prejuízos consideráveis para as empresas ao nível financeiro, designadamente quando estamos a falar da interrupção do negócio, perda de informação e até danos ao nível da reputação que, em última instância, podem levar ao encerramento das empresas.

Há uma preocupação acrescida desde que foi implementado, a 25 de Maio deste ano, o novo Regulamento Geral da Proteção de Dados que trouxe a necessidade das empresas implementarem uma série de medidas e políticas adicionais relativamente a estas matérias. As multas por incumprimento são elevadíssimas, podendo chegar a 20 milhões de euros ou 4% do volume de faturação no conjunto das jurisdições onde opera, optando-se, entre estes dois, pelo valor que for mais elevado. Por tudo isto, efetivamente, nos dias que correm, deve ser uma preocupação crescente e constante a segurança informática nas empresas.

Como é que as empresas se podem proteger de riscos cibernéticos?

As empresas devem, em primeiro lugar, fazer uma avaliação e quantificação dos riscos, procurar fazer uma gestão preventiva desses mesmos riscos, e delinear um plano de resposta para este tipo de incidentes. Outra forma que as empresas têm de se proteger é através da contratação de seguros de riscos cibernéticos. É uma

forma de transferir esses riscos para as seguradoras e, assim, mitigar o risco das empresas. Em regra, este tipo de seguros disponibiliza aconselhamento jurídico para um plano de ação, bem como pessoal técnico especializado ao nível da segurança informática. Ao nível da cobertura, estes seguros cobrem não só situações de responsabilidade civil da empresa, bem como os custos associados à recuperação dos dados, ao nível de investigações que sejam precisas desencadear relacionadas com o ataque, multas que possam existir, também ao nível de relações públicas quando seja necessário a contratação destes serviços para redução ao máximo de eventuais danos reputacionais e, portanto, cobre uma série de custos que estão associados a este tipo de incidentes.

Perante um ataque cibernético que devem as empresas fazer?

O ideal, efetivamente, é a prevenção. Procurar aconselhamento jurídico para saber se, efetivamente, as medidas implementadas estão de acordo com a legislação de proteção de dados em vigor, bem como se a contratação do seguro de riscos cibernéticos é, efetivamente, a que melhor se adequa à realidade da empresa. Mas perante um ataque cibernético, havendo seguro, a empresa deve acionar imediatamente o seguro porque, quase sempre, este disponibiliza equipas 24 horas por dia que recebem pedidos de auxílio nestas situações e permite, não só, acesso a pessoal especializado em segurança informática, bem como o já mencionado aconselhamento jurídico para que seja delineado um plano de ação. Não havendo seguro, a empresa deve procurar, de imediato, ajuda especializada no sentido de fazer um diagnóstico da situação por forma a tentar bloquear e avaliar os eventuais danos, bem como iniciar os procedimentos de recuperação de dados necessários de imediato. Outra forma de prevenção é a análise dos riscos que esse incidente pode desencadear, designadamente através da avaliação do ponto de vista jurídico de riscos e contraordenações aplicáveis por não conformidade com a lei, bem como eventual responsabilidade civil que daí advenha. Perante essa informação, a empresa estará em melhores condições para poder delinear um plano de ação para mitigar riscos associados a uma situação concreta. É fundamental também o apoio jurídico para efeito das notificações e comunicações necessárias em caso de violação de dados pessoais, não só à Comissão Nacional da Proteção de Dados bem como aos titulares desses dados pessoais de acordo com o Regulamento. E, por exemplo se estivermos perante um caso em que a empresa está perante um crime informático, o apoio jurídico é também importante ao nível da apresentação da respetiva denúncia, procurar preservar a prova ao máximo, que é necessária para efeitos do processo-crime, bem como para acompanhamento deste procedimento. ●