IT Channel
Informação essencial para VARs e Integradores de tecnologia

01-06-2016

Tiragem: 2150
País: Portugal
Period.: Mensal
Âmbito: Tecnologias de Infor.

Pág: 31
Cores: Cor
Área: 23,38 x 27,53 cm²
Corte: 1 de 1

Inês de Castro Ruivo | Associada da Área de TMT de PLMJ

E se os "Panama Papers" tivessem acontecido em Portugal?

Mais de 11,5 milhões de documentos confidenciais da sociedade de advogados Mossack Fonseca, sedeada no Panamá, foram divulgados no passado mês de abril, naquela que já é a maior fuga de informação da história, mil e quinhentas vezes maior do que a Wikileaks

Os números dizem tudo: 2,6 terabytes de dados que abrangem a atividade da sociedade durante cerca de 45 anos e que, se não fosse através da Internet, nunca seriam acedidos e disponibilizados a esta escala. Estima-se que seriam necessárias 2.600 carrinhas *pick up* para, fora do mundo digital, transportar toda esta informação para fora dos muros da Mossack Fonseca. Para o *hacker* que entrou nos sistemas desta empresa a tarefa foi certamente astuciosa, mas bem menos pesada.

O que aconteceu à Mossack Fonseca pode acontecer a qualquer empresa portuguesa. Quanto mais sensível for a informação detida pela empresa, mais apetecível é o acesso à mesma. Bancos, sociedades de advogados e empresas que tratem dados sensíveis de clientes poderão ser alguns dos alvos preferidos, mas os mais recentes números mostram que qualquer empresa pode ser vítima de um ciberataque[1].

Como reagir contra um *data breach*?

A Lei do Cibercrime, em vigor em Portugal, pune o acesso ilegítimo a sistemas informáticos com pena de prisão até um ano. Esta pena poderá ir até aos cinco anos de prisão, quando o acesso tenha permitido ao agente do crime tomar conhecimento de segredos comerciais ou industriais ou dados confidenciais, ou lhe tenha permitido obter benefícios patrimoniais de valor consideravelmente elevado.

No caso dos Panama Papers, não se conhece a identidade do *hacker* que protagonizou a fuga massiva de informação, nem se sabe tão pouco se esta fuga terá sido um inside job, levado a cabo por um advogado ou funcionário da empresa, ou se terá sido perpetrada por alguém do exterior.

Em Portugal, a revelação ou divulgação de dados pessoais levada a cabo por alguém obrigado a sigilo profissional poderá ser punida com pena de prisão até dois anos. É o caso dos advogados, técnicos oficiais de contas e contabilistas, entre outros. A pena será ainda mais pesada se o agente for um funcionário público ou se a sua ação for movida pelo interesse de obter vantagens patrimoniais ou outros benefícios e, ainda, se a divulgação puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.

Quais as consequências para a empresa?

É certo que a divulgação pública da ocorrência de uma falha de segurança pode afetar a reputação da empresa no mercado e junto dos seus clientes, podendo implicar a responsabilidade civil da mesma. A ocorrência de um evento deste tipo poderá ainda provocar a interrupção do negócio, com todas as consequências financeiras daí advenientes.

Atualmente, a Lei da Proteção de Dados Pessoais não obriga as empresas que sofram um data breach a notificar esta ocorrência aos seus clientes e às autoridades. Esta obrigação vigora atualmente apenas para as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público.

No entanto, esta realidade vai mudar. O novo Regulamento europeu relativo ao tratamento de dados pessoais, publicado no passado mês de maio e que entrará em vigor em 2018, consagra expressamente a obrigação de a empresa notificar a Comissão Nacional de Proteção de Dados e, em certos casos, os cidadãos afetados.

Prevenir continua a ser o melhor remédio

A informação tornada disponível no caso Panama Papers indicia que os e-mails trocados entre os advogados da Mossack Fonseca e os respetivos clientes não eram encriptados, o que coloca algumas dúvidas sobre a robustez das medidas de segurança adotadas.

Para além da adoção de medidas de segurança adequadas, as empresas podem – e devem – sensibilizar os seus trabalhadores para os riscos, ainda que não intencionais, das falhas de segurança. A implementação de políticas de segurança e políticas de tratamento de dados pessoais é uma das formas de prevenção, permitindo minorar os riscos de um data breach com origem interna.

Quanto a ataques externos, prevenir continua a ser o melhor remédio e, para quem o desempenha, uma verdadeira "never ending story".

[1] *Segundo uma notícia publicada no Diário de Notícias em 2 de outubro de 2015, a Polícia Judiciária registou 850 ciberataques em 2015*