Valores, Ética
e Responsabilidade

Admirável mundo novo: o cibercrime

Mais de 35% das empresas incluem o risco associado à cibercriminalidade no Top 5 dos riscos a gerir em 2017. Mas uma grande parte não tem mecanismos de gestão de risco que permitam responder a situações inesperadas, como aqueles que decorrem de ataques cibernéticos. E, em geral, as empresas sabem relativamente pouco sobre os riscos inerentes à cibercriminalidade

POR SOFIA RIBEIRO BRANCO E ANA LOURENÇO

A consultora Marsh acabou de divulgar um estudo segundo o qual mais de 35% das empresas incluem o risco associado à cibercriminalidade no Top 5 dos riscos a gerir em 2017. O mesmo estudo mostrou, contudo, que uma parte ainda grande das empresas não tem mecanismos de gestão de risco que permitam responder a situações inesperadas, como aqueles que decorrem de ataques cibernéticos. Por outro lado, em geral, as empresas sabem relativamente pouco sobre os riscos inerentes à cibercriminalidade.

Com efeito, as empresas estão cada vez mais expostas à intrusão indesejada nos seus sistemas informáticos sem que, na sua maioria, estejam sensibilizadas para os perigos da cibercriminalidade e para as medidas a tomar para prevenir a sua ocorrência ou reagir a ciberataques ou a 'ciber-incidentes'.

O objectivo deste artigo é, precisamente, o de contribuir para começar a desbravar o caminho das empresas para a prevenção e a protecção relativamente ao cibercrime, através da resposta às seguintes questões fundamentais: O que é o cibercrime? Que relevância tem hoje em dia? Como podem as empresas lidar com os riscos do cibercrime? E como devem actuar caso suspeitem ser alvo de cibercrime?

Habitualmente, falamos de cibercrime para designar a prática de crimes através de computadores e, em particular da Internet, embora a expressão inclua várias categorias de crimes muito diferentes, nomeadamente:

Sofia Ribeiro Branco, Partner da Vieira de Almeida
e Ana Lourenço, Assistant Professor da Católica Porto Business School

- Crimes em que o computador é o instrumento da prática criminosa, ou seja, crimes que, não sendo novos, passam a ser cometidos com o auxílio de computadores e de redes electrónicas de comunicação (como, por exemplo, os crimes de devassa por meio de informática, de burla informática e de burla nas comunicações, previstos no Código Penal);
- Crimes informáticos propriamente ditos, em que o computador é o alvo da prática criminosa (como, por exemplo, os crimes de falsidade informática, sabotagem informática e acesso ilegítimo a sistema informático, previstos na Lei do Cibercrime);
- Crimes relacionados com conteúdo ilícito online (como, por exemplo, a difusão de pornografia infantil e o incitamento à violência, ao racismo, à xenofobia ou ao terrorismo);
- Crimes que correspondem a práticas que violam a protecção de dados e a privacidade das pessoas.

A cibercriminalidade é, naturalmente, muito potenciada pela Internet. É verdade que a Internet nos permite armazenar e ter acesso a numerosa informação, comunicar com qualquer pessoa e concretizar transacções

em qualquer parte do mundo. Porém, também nos expõe, mesmo que involuntariamente, e pode, em caso de ciberataque, pôr de tal forma em causa a nossa privacidade que se torna um instrumento temido e susceptível de causar danos patrimoniais e morais.

Com o aumento da capacidade das redes electrónicas e o acesso generalizado à Internet a partir de plataformas tão diversas quanto o computador, o tablet ou o smartphone, o cibercrime tem aumentado ao longo dos anos. Ao número crescente de crimes junta-se a capacidade inventiva dos ciberatacantes (ou *hackers*), que a cada dia vão concebendo e partilhando em comunidades informais novas práticas criminosas. Veja-se, por exemplo, o caso do *ransomware*, considerada a maior ameaça virtual de 2016: o ciberatacante adquire o controlo do computador de outra pessoa e exige um resgate pela devolução do controlo, praticando assim, agora através de um computador, o crime de extorsão.

Ao número crescente de crimes junta-se a capacidade inventiva dos ciberatacantes

O aumento da cibercriminalidade justificou que o Ministério Público a elegesse – a par com a prova digital – como área prioritária de acção em 2015-2016. Contudo, a investigação do cibercrime debate-se com diversas dificuldades: desde logo, o criminoso ataca à distância, de forma anónima e dispersa a informação; as suas acções atingem um grande número de vítimas, muitas vezes em escassos segundos, e a partilha das novas práticas criminosas induz a globalização dos ataques, exigindo das autoridades rapidez na actuação, uma intensa cooperação e recursos humanos especializados.

Estas dificuldades na investigação dos cibercrimes, associadas às revelações que são trazidas a público através dos ciberataques têm, nalguns casos, colocado o foco não tanto na perseguição dos criminosos, mas na utilização dos elementos obtidos através da intrusão nos sistemas informáticos. Pensemos, por exemplo, nos casos Panama Papers e Luxleaks, nos quais a atenção acabou por recair mais na investigação dos crimes fiscais indiciados do que na busca ou punição dos ciberatacantes.

Para as empresas, são vários os riscos associados ao cibercrime: furto de dados dos clientes, dos colaboradores e da própria empresa com inerente prejuízo para o negócio e, por vezes, para a reputação ou com interrupção da actividade em virtude de ataques de vírus.

Para prevenir eventuais ciberataques, cabe à empresa criar regras internas de gestão do risco de ciberataque, designadamente regras relativas à utilização da Internet no local de trabalho. São exemplo destas regras as relativas à utilização e alteração de passwords, ao acesso a determinados sites, à instalação e actualização de antivírus, à reacção face a emails suspeitos e à gravação de ficheiros. Devemos referir também a

existência de seguros que cobrem os riscos de ciberataques, cuja subscrição deve ser ponderada pelas empresas.

No caso de algum gestor ou colaborador de uma empresa suspeitar que esta foi vítima de um cibercrime, há algumas medidas que devem ser tomadas. Desde logo, é crucial reportar às autoridades o ciber-incidente com a maior celeridade, para que seja possível acautelar a prova dos factos e perseguir os criminosos. A suspeita deve ser reportada às autoridades, designadamente ao Gabinete do Cibercrime, que funciona na dependência da Procuradoria-Geral da República, e à Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica, uma estrutura da Polícia Judiciária. Alguns dos tipos de cibercrime estão dependentes de queixa, que deve ser apresentada no prazo de seis meses a contar da data em que o titular da queixa tiver conhecimento do facto e dos seus autores.

É importante referir também que, a partir de Maio de 2018, será directamente aplicado em Portugal o Regulamento Geral sobre Protecção de Dados, com obrigações relevantes para as empresas no que respeita à mitigação dos riscos de ataques a dados pessoais e às medidas a implementar para prevenir e reagir a ciber-incidentes.

Em conclusão, nos tempos que correm todos temos de estar atentos ao modo como utilizamos os computadores e as redes informáticas, em particular a Internet, e nos protegemos nesta utilização. Os riscos de ciberataques podem ser reduzidos, se forem geridos com cuidado e no interesse não só individual, mas empresarial e colectivo.

Source: http://www.ver.pt/admiravel-mundo-novo-o-cibercrime/