CRÓNICA VISÃO ELECTRÓNICA
Nº 215 / 2013-02-28
http://www.gestaodefraude.eu
Elisabete Maciel

>> Segurança da informação: a ilusão

Se trancamos as nossas portas, porque não proceder da mesma forma em relação aos dispositivos electrónicos móveis que utilizamos no nosso dia a dia?

No mundo empresarial contemporâneo as empresas manipulam e armazenam uma grande quantidade de informação vital para a sua sobrevivência. Tendo em conta o desenvolvimento vertiginoso das tecnologias de informação, associado à obrigatoriedade da partilha de informação com todos os envolvidos no negócio, as empresas, nos dias que correm, facilitam cada vez mais o acesso à sua informação através do mais variado tipo de dispositivo: portáteis, *tablets*, *smartphones*, etc. Será que as empresas têm a noção dos riscos em que incorrem ao abrirem a sua rede a todo o tipo de dispositivos? Estarão elas preparadas para garantir a segurança da sua informação?

Alguém afirmava que a única rede segura é aquela que não tem pessoas a ela ligadas…

Consideremos uma situação que poderia perfeitamente ocorrer na realidade. Uma empresa equipou os seus funcionários com *smartphones* tendo em vista permitir-lhes o acesso, em qualquer momento e em qualquer lugar, à informação empresarial. Como tal, estes dispositivos armazenam todos os contactos úteis, permitindo o acesso aos mails relacionados com a sua actividade laboral. Um funcionário recebe uma SMS, que em tudo parece vir da sua empresa, solicitando que faça o download de uma nova aplicação a instalar no seu *smartphone*. Ao receber essa mensagem, que não duvida seja verdadeira, procede à sua instalação. Na realidade, trata-se de uma mensagem fraudulenta que pretende instalar um software malicioso (*malware*). Ademais, o dispositivo telefónico não apresenta quaisquer sinais de ter ficado infectado. No entanto, o autor do *malware* passou a ter controlo remoto sobre o dispositivo, o que lhe permite, por exemplo, interceptar todas as chamadas e mensagens, aceder à lista de contactos ou até activar à distância o gravador e passar a ter acesso às conversas que decorram, por exemplo, numa reunião de trabalho.

CRÓNICA VISÃO ELECTRÓNICA
Nº 215 / 2013-02-28
http://www.gestaodefraude.eu
Elisabete Maciel

De acordo com dados publicados pelo Banco Mundial (Information and Communications for Development - 2012) de 2005 a 2011 o número de telefones móveis vendidos em todo o mundo passou de 800 para 1800 milhões. Nesse mesmo período, a venda de *smartphones* praticamente decuplicou (de 50 para 470 milhões). Embora não haja informação acessível sobre o número de smartphones vendidos em Portugal, tudo leva a crer que a situação será, no mínimo, idêntica. De acordo com o mesmo relatório e para 2011, o número de subscrições de telefones móveis por 100 habitantes em Portugal(158) é significativamente superior ao verificado para o grupo de países em que está incluído (elevado rendimento). Neste grupo, o valor é de 118 subscrições por cada 100 habitantes.

O aumento exponencial de *smartphones* no mercado e a política de redução de custos muitas vezes adoptada pelas empresas, materializada no consentimento da utilização dos dispositivos que são pertença dos funcionários (BYOD – *Bring your Own Device*) para uso laboral, mantém a premência da discussão em torno das questões relacionadas com a segurança da informação. Por outro lado, a preocupação que ao longo dos últimos anos existiu em proteger minimamente os computadores utilizados no local de trabalho perante possíveis ataques, não se tem estendido aos *smartphones*. No entanto, existem várias soluções no mercado para os protegerem. Verifica-se, todavia, que as pessoas ou não as conhecem ou acham que a sua utilização degrada o desempenho do seu smartphone e, consequentemente, ignoram-nas.

No mínimo, exigia-se que "antes da casa roubada pusessem trancas à porta"... Sendo assim, era expectável que impedissem o acesso à informação armazenada no *smartphone* utilizando uma *password*. Este procedimento básico permitia, pelo menos, minimizar os estragos que poderiam resultar de um possível roubo. Em relação às restantes ameaças, o melhor conselho é pensar em instalar uma aplicação que garanta a segurança da informação. De notar que estas aplicações permitem, entre outras acções, bloquear remotamente o dispositivo através dum simples SMS e, numa situação extrema apagar toda a informação armazenada no *smartphone*. Para tal, basta utilizar um computador com acesso à Internet.

Não esquecer que, regra geral, o dono de um *smartphone* é o prin-

CRÓNICA VISÃO ELECTRÓNICA
Nº 215 / 2013-02-28
http://www.gestaodefraude.eu
Elisabete Maciel

cipal responsável por o infectar, quer seja através da instalação de uma aplicação maliciosa, quer seja pela simples operação de efectuar o download de um jogo a partir de um site não fidedigno.

É chegado o momento das empresas olharem para a realidade e mudarem de atitude. A maior parte dos incidentes de segurança da informação têm origem internamente sendo que, muitos deles seriam perfeitamente evitáveis.