**24 - Segurança em dispositivos móveis**

Autor: CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática

Os dispositivos móveis são usados não apenas para guardar informação pessoal mas, muitas vezes, para armazenar informação mais sensível, como notas de reuniões de trabalho ou documentos internos de organizações. Tendo em conta a quantidade de informação que estes dispositivos podem conter, devemos ter um particular cuidado com eles.

Em primeiro lugar, a proteção de ecrã do dispositivo deverá estar ativa. Vários dispositivos permitem que seja definida uma palavra-passe usada para acesso ao dispositivo. Isto que faz com que, em caso de perda, a pessoa que o encontrar não possa ter fácil acesso à informação. Devem igualmente ser preenchidos os detalhes de contacto pessoal, para que uma pessoa que encontre o telemóvel possa proceder à devida devolução.

Se existir informação particularmente sensível, como calendários com agendamento de reuniões de trabalho ou outros, deve ser ativada a funcionalidade de remoção remota de conteúdos. Existem algumas aplicações/serviços gratuitos para os diversos tipos de dispositivos que permitem, em caso de perda ou roubo do dispositivo, apagar todos os dados em questão de uma forma remota. Deste modo, a pessoa que encontrar um telemóvel ou *tablet* perdido, dificilmente terá acesso aos dados que estes podem conter. No caso do dispositivo ser um Android, aplicações possíveis para esse fim são a Mobile Defense ou WaveSecure; para iPhone existem aplicações como Find My iPhone ou MobileMe.

Caso tenha o hábito de efetuar cópias de segurança do seu dispositivo, tem de ter um particular cuidado com elas, pois estas cópias contêm em si todas as palavras-passe guardadas no dispositivo. O acesso às cópias permite assim que um atacante possa aceder a informação pessoal (como o histórico de todos os sites visitados) e, por essa razão, a uma enorme quantidade de informação sobre o proprietário do dispositivo. Guardar as cópias de forma cifrada (há quem use o neologismo “encriptada”) com uma palavra-passe forte é uma boa prática aconselhada.

Aquando da instalação de aplicações no dispositivo deve sempre ter atenção ao tipo de permissões que estas solicitam. Se uma aplicação que à partida não tem de aceder ao e-mail pedir permissões para aceder às contas configuradas é de desconfiar e, se possível, deve arranjar outra alternativa a essa aplicação.

---------------------------------------------------------------------------

**Mês Europeu da Cibersegurança**

Este artigo é da autoria de especialistas do CERT.PT- Serviço de Resposta a Incidentes de Segurança Informática (www.cert.pt) da FCCN-Fundação de Computação Científica Nacional (www.fccn.pt/pt) e insere-se na campanha "Uma dica por dia" integrada no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013.

O Mês Europeu da Cibersegurança é uma iniciativa da ENISA - Agência Europeia para a Segurança das Redes e Informação (www.enisa.europa.eu) e o seu objectivo é informar os utilizadores sobre a importância da segurança da informação, bem como demonstrar algumas medidas simples para proteger os seus dados.

----------------------------------------------------------------------------

**Nota aos editores da Imprensa regional**

Os artigos da autoria dos técnicos do CERT.PT incluídos no Mês Europeu da Cibersegurança, que tem lugar em Outubro de 2013, surgem no site da Ciência na Imprensa Regional numerados, de forma a permitir a sua mais fácil identificação. No entanto, eles são absolutamente independentes uns dos outros e podem ser publicados pelos órgãos de comunicação de forma avulsa.

------------------------------------------------------------------------------

Foto de Tetiana Vitsenko

(Existem ficheiros de imagem de mais alta resolução disponíveis para download)