**25 - Segurança na Cloud**

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

Nos últimos anos temos usado cada vez mais a “Cloud” para guardar os nossos dados. Chamamos “Cloud” a um conjunto de serviços existentes na Internet, sem uma localização fixa, e muitas vezes distribuídos por inúmeros servidores e fornecidos por diferentes empresas. Os serviços Cloud oferecem-nos armazenamento de dados com redundância e aplicações que, em vez de estarem instaladas no nosso computador, existem apenas “na Internet”, e podem ser utilizadas online.

Guardamos na Cloud fotos, notas, trabalhos ou até documentos sensíveis e esperamos que a empresa que providencia o serviço guarde os nossos ficheiros de forma segura.

É importante recordar que, mesmo quando guardamos ficheiros na Cloud, os primeiros responsáveis pela segurança da informação somos nós. Se usamos uma palavra-chave fraca, facilmente um atacante terá acesso aos nossos dados sem ter de comprometer o sistema da empresa onde estes estão guardados. Ao guardar ficheiros na Cloud devemos escolher sempre uma palavra-passe forte.

Quando usamos estes serviços, devemos partir do princípio de que a própria empresa onde estão guardados os ficheiros pode ter acesso aos mesmos. Os colaboradores destas empresas podem ter acesso às pastas onde estão guardados todos os nossos ficheiros e, em certas circunstâncias, as empresas podem ser obrigadas a entregar esses dados a autoridades judiciais.

Se guardarmos informação sensível nestes serviços, devemos usar uma aplicação de cifra (a que algumas pessoas chamam de “encriptação”) para criar uma pasta segura dentro da nossa área na Cloud e usar uma palavra-passe forte para aceder à informação. Com esta proteção, nem mesmo os colaboradores da empresa de alojamento terão acesso aos seus dados.

Existem várias aplicações que podemos usar para cifrar dados. Para a grande maioria dos sistemas operativos é possível usarmos a aplicação gratuita TrueCrypt, que cria proteção extra para os documentos mais sensíveis.

Nos serviços que o permitam, como o GMail ou Outlook, por exemplo, é de considerar ativar uma autenticação que recorre a uma dupla chave: a sua palavra-chave habitual e uma outra que é gerada dinamicamente e que lhe pode ser enviada por SMS ou e-mail.

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

**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 Jakub Jirsák

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