**29-Cibersegurança e infra-estruturas críticas**

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

Proteção de infra-estruturas críticas é o conjunto de meios e técnicas que proporcionam a segurança dos activos considerados essenciais para o bom funcionamento de funções críticas da sociedade, incluindo a cadeia de fornecimento, a saúde, a protecção, a segurança e o bem-estar económico e social da população. Essa proteção deve ter como pano de fundo um conjunto de ameaças no qual se inlcuem os ciberconflitos.

Infra-estruturas como por exemplo os serviços de saúde, as comunicações, o fornecimento de água e energia, a distribuição de alimentos, os serviços de emergência ou os serviços financeiros são consideradas áreas críticas em Portugal devido à sua importância para a segurança dos cidadãos, para a actividade económica e para o dia-a-dia da população.

Analisando os problemas que alguns países da União Europeia já enfrentaram a este nível e a forma como os tentam prevenir, verificamos que muitos deles têm reforçado os seus investimentos na segurança das suas infra-estruturas. O caso do ciberataque à Estónia, em 2007, é um exemplo bem estudado. Este país enfrentou uma série de ataques a sites de organizações como o parlamento, bancos, polícia e meios de comunicação, deixando os respetivos serviços indisponíveis para a população durante vários dias. O governo estónio atribuiu a responsabilidade dos ataques à Rússia, com quem o país estava envolvido numa disputa diplomática, mas a sua autoria nunca chegou a ser provada. Os especialistas de cibersegurança atribuem os incidentes a uma série de grupos de *hackers* organizados.

No sentido de promover a cibersegurança a nível nacional, incluindo em sectores relativos a infra-estruturas críticas do país, nos últimos anos, o CERT.PT tem vindo a dinamizar uma rede nacional de CSIRTs (Rede de Equipas de Resposta a Incidentes de Segurança - uma espécie de bombeiros da Internet) que integra já cerca de 20 equipas de sectores importantes da sociedade como os prestadores de serviços de comunicações electrónicas, sectror energético e o sector financeiro. Partindo do principio de que é preciso trabalhar em rede para responder a ameaças organizadas na rede, o principal objectivo da Rede Nacional de CSIRTs é criar um ambiente de cooperação e assistência mútua no tratamento de incidentes e na partilha de boas práticas de segurança.

No seio desta rede foi desenvolvido um conjunto de instrumentos que permitem uma melhor coordenação da resposta a incidentes de segurança de grande dimensão, nomeadamente a definição de uma taxonomia comum, um formato para partilha de informação, mecanismos de comunicação segura e um conjunto de boas práticas de actuação para as tipologias de incidentes mais comuns. Outra responsabilidade dos membros desta rede é a disseminação de boas práticas sobre a utilização segura das TIC junto dos cidadãos.

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

**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 xx

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