**26 - Estratégia europeia de Cibersegurança**

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

Em fevereiro de 2013, a Comissão Europeia, em colaboração com a Alta Representante da União para os Assuntos Estrangeiros e Política de Segurança, publicou um documento de estratégia em matéria de cibersegurança e uma proposta de diretiva sobre a segurança das redes e da informação.

Com o título “Um ciberespaço aberto, seguro e protegido”, o Plano de Cibersegurança da UE expõe a visão da União Europeia sobre a melhor forma de prevenir e defender as perturbações e ataques no ciberespaço europeu. O documento define medidas que visam o aumento da resiliência dos sistemas informáticos, o recuo da cibercriminalidade e o reforço da política internacional da EU em matéria de cibersegurança e ciberdefesa.

Esta estratégia assenta sobre cinco pilares:

* Desenvolver a política e as capacidades no domínio da ciberdefesa no quadro da Política Comum de Segurança e Defesa (PCSD)
* Reforçar meios de prevenção e oposição a ataques
* Desenvolver recursos industriais e tecnológicos em matéria de cibersegurança
* Reduzir drasticamente a cibercriminalidade
* Estabelecer uma política internacional coerente no ciberespaço para a União Europeia e promover os seus valores fundamentais

Uma das orientações principais deste plano é obrigar os estados-membros a designar uma autoridade nacional competente para a cibersegurança, com recursos financeiros e operacionais e capacidade de gestão no tratamento de incidentes de segurança informática, a qual serviria de ponto de contato no tratamento de incidentes transfronteiriços.

Outra medida preconizada é a criação de mecanismos seguros que facilitem uma maior cooperação entre estados-membros na difusão dos alertas e respostas a incidentes informáticos e permitam a coordenação de intervenções conjuntas.

O plano estratégico visa igualmente um maior envolvimento na cibersegurança por parte das empresas cujo negócio assenta sobre plataformas web: operadores de infraestruturas críticas tais como energia, saúde, serviços financeiros, transporte e administração pública. Esse envolvimento passaria pela adoção de medidas que impliquem a obrigação de notificação de incidentes críticos bem como a implementação de boas práticas em matéria de gestão de risco.

Pode consultar o Plano de Cibersegurança da UE aqui: <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667>

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

**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 Marina Strizhak

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