Notas da Intervenção do Presidente da UMIC – Agência para a Sociedade do Conhecimento, IP Luis Magalhães, no 1º Seminário de Equipas de Resposta a Incidentes de Segurança de Computadores, 10.11.2010

A UMIC – Agência para a Sociedade do Conhecimento, IP tem por missão **coordenar as políticas para a sociedade da informação** e mobilizá-la através da promoção de actividades de divulgação, qualificação e investigação, **promover o desenvolvimento tecnológico e a criação de conhecimento** por entidades do sistema científico e tecnológico e por empresas, e **estimular o desenvolvimento da e-Ciência**, isto é, das Tecnologias de Informação e Comunicação (TIC) como instrumentos para a actividade científica. Uma das suas atribuições é promover a cibersegurança e a privacidade no uso da Internet e das (TIC).

É a partir desta perspectiva que faço a presente intervenção. Como entidade financiadora da FCCN – Fundação para a Computação Científica Nacional quero felicitar a FCCN pela organização deste seminário sobre o importante tema das Equipas de Resposta a Incidentes de Segurança de Computadores (CSIRSTs), e em especial a equipa do **CERT.PT** da FCCN directamente envolvida nos aspectos práticos de organização e que foi a primeira CSIRT a funcionar em Portugal (desde 2000), a ser acreditada internacionalmente (desde Março de 2004) e a única acreditada internacionalmente até 2007 quando também ficou acreditada a CSIRT da Faculdade de Engenharia da Universidade do Porto..

A segurança informática é um factor crítico para os sistemas e informação e comunicação, logo praticamente para todos os sectores económicos e de actividade humana. Como em todas as outras áreas de actividade humana, **os desafios são principalmente organizacionais e de capacitação humana, e não simplesmente tecnológicos ou policiais**.

As promessas da **Internet do Futuro**, das **redes de sensores e actuadores distribuídos**, da **computação em nuvem** *(cloud computing)*, dos **ambientes interactivos e inteligentes**, da **ubiquidade dos sistemas informáticos** e de poderosos **aparelhos e comunicações móveis**, tornarão **ainda mais exigentes os requisitos de segurança informática**.

As preocupações de segurança assumem importância aos vários níveis da Internet e dos sistemas informáticos:

- **Na camada de infraestrutura**, através da segurança física de equipamentos e instalações, da segurança de redes dedicadas a funções críticas.

- **Na camada de protocolos de comunicação**, através de encriptação, certificados de identidade, sistemas tipo DNSSEC para certificação da verdadeira identidade de um domínio e de Roteamento Seguro com base nos sistemas de Certificação de Recursos *(Resource Routing/Route Origin Authorization (ROA))* como os que os *RIRs –Regional Internet Registries* dos cinco continentes vão pôr em produção em 1 de Janeiro de 2011.

- **Na camada de aplicações**, através da segurança por projecto *(security by design)*, do uso de certificados de identidade e de encriptação.

- **Na camada de organização**, através de procedimentos de segurança, de aquisição de equipamentos e aplicações com requisitos de segurança adequados, de gestão de risco de segurança, de operação articulada de uma rede de CSIRTs, de exercícios de segurança *tipo cyber storm,* de levantamento de vulnerabilidades e definição de procedimentos de protecção de infraestruturas críticas.

Assim, este seminário é muito oportuno. O esclarecimento de como deve ser organizada a cooperação entre CSIRTs, tanto em âmbito nacional como internacional, é essencial para um destes níveis da segurança informática.

Um aspecto essencial é que tem de haver um permanente bom equilíbrio entre segurança e liberdade/privacidade/facilidade de uso. Os requisitos limitativos da utilização fácil e livre por razões de segurança devem ser sempre os mínimos absolutamente necessários em cada situação particular e deve ser sistematicamente evitado a adopção de normas de segurança máxima para tudo, mesmo para actividades que não necessitam desses níveis de segurança. Deve ser seguido um princípio de proporcionalidade entre medidas de segurança e os riscos envolvidos. A este propósito cabe mencionar a questão específica da autenticação de entidades em que há frequentemente a tendência de adoptar sistemas de autenticação forte de identidade informática, com certificados digitais qualificados ou dados biométricos, quando a maior parte das situações não exige este nível de autenticação de identidade e pode, e em certos casos deve, funcionar bem com sistemas de autenticação assertiva por nomes de utilizadores e *passwords* ou até com anonimato. Aqui também, o princípio de nível mínimo de controlo de identidade deve ser adoptado.

É preciso notar que há três requisitos básicos que têm efeitos transversais em todos os níveis que referi:

- **Investigação e Desenvolvimento (I&D).** A contribuição central para todas as camadas é de novo conhecimento, novos sistemas, nova tecnologia. A dimensão da **Internet do Futuro** com milhares de milhões de utilizadores, com dezenas de milhares de milhões de aparelhos comunicantes, centenas de milhares de milhões de sensores comunicantes, milhares de milhões de milhões de etiquetas de identificação informática em objectos, a grande maioria dos quais interligados pela Internet, exige soluções baseadas em novos conhecimentos e tecnologias desenvolvidos com base em I&D. A

complexidade e a dimensão dos problemas é incompatível com a utilização pura e simples de sistemas de segurança não baseados em I&D.

A natureza resolveu problemas de segurança de informação e comunicação muito mais complexos e de maior dimensão do que os que temos presentemente nos sistemas informáticos, como são por exemplo a transmissão, replicação e reparação de DNA, o sistema imunológico, a transmissão e processamento neuronal. Inclusivamente haverá muito a aprender com estes sistemas naturais em termos da I&D em segurança informática.

- **Educação e Formação.** É necessário assegurar a adopção de currículos de educação actualizados no Ensino Superior, que confiram conhecimento ao nível do estado-da-arte, e é necessário assegurar as oportunidades de formação ao longo da vida em segurança informática.

- **Cooperação Internacional.** Sendo o ciberespaço desmaterializado e com expressão global, a segurança informática tem de ser prosseguida em forte cooperação internacional.

A segurança policial e o controlo de qualidade, embora necessários como em outros aspectos da vida em sociedade, não são os aspectos essenciais da segurança informática. **Os sistemas que se baseiem principalmente em segurança policial e em sistemas de controlo de qualidade e que negligenciem a I&D e a Educação e Formação acabarão por falhar redondamente!**

Finalmente, umas palavras sobre a **constituição de uma CSIRT na Administração Pública**. Este objectivo deveria ser prosseguido, tirando partido da experiência do CERT.PT da FCCN no que respeita a definição de procedimentos e formação de técnicos. O CERT.PT continuaria a assumir uma acção de âmbito nacional fora da administração pública e asseguraria a relação com o público geral e as empresas tirando partido da FCCN assegurar a gestão do DNS sob .pt e do *Internet Exchange Point* português que interliga o tráfego dos ISPs (GigaPix) bem como a gestão da 1ª Rede de Nova Geração *(NGN – Next Generation Network)* a funcionar em Portugal, designadamente a RCTS – Rede Ciência Tecnologia e Sociedade que serve o sistema científico e de ensino superior nacional e mantém um amplo leque de serviços avançados sobre banda larga em funcionamento. Na Administração Pública em Portugal, seria constituída uma única CSIRT, dirigida para os organismos da administração pública, eventualmente completada apenas com uma outra no âmbito das entidades da Defesa Nacional, devido aos custos envolvidos e a não ser necessário multiplicar este tipo de entidades. **Seria desejável que a CSIRT da Administração Pública fosse gerida em rede, com recursos humanos distribuídos nos principais centros informáticos da Administração Pública** (Modernização Administrativa, Rede Informática do Governo, Finanças, Administração Interna, Justiça).

Concluindo, faço votos que esta jornada de trabalho seja produtiva para a troca de experiências entre os participantes e contribua para a clarificação do papel e organização dos CSIRTs em Portugal e para a colaboração entre estas entidades em Portugal e internacionalmente.

Muito obrigado pela vossa atenção.