**27 - A importância do DNSSEC**

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

DNSSEC é o nome dado às extensões de segurança ao protocolo DNS (Domain Name System) concebidas para proteger e autenticar o tráfego DNS. O protocolo DNS, basicamente, o que faz é traduzir endereços do tipo [www.nome.pt](http://www.nome.pt), que são fáceis de memorizar e que escrevemos na barra de endereços do nosso *browser*, num endereço numérico, o endereço IP ou “o número de telefone” do *site* a que se pretende aceder.

Os mecanismos de segurança previstos no DNSSEC são complementares e transparentes para o utilizador, não interferindo com o normal funcionamento do protocolo DNS. O DNSSEC foi criado para responder às preocupação de segurança dos utilizadores nas transações eletrónicas e veio mitigar uma série de vulnerabilidades e de vetores de ataque bem conhecidos, nomeadamente:

* Supressão de fragilidades do protocolo DNS
* Prevenção de alguns ataques específicos (*man-in-the middle* e *cache poisoning)*
* Redução do risco de manipulação de informação
* Reforço da fiabilidade do sistema

O sistema de nomes de domínio (DNS) é uma das ferramentas fundamentais para o funcionamento da Internet. Para além de permitir ao utilizador ignorar os endereços de IP, permite alterações desses endereços IP sem que o utilizador tenha que as conhecer para continuar a usar um serviço. O sistema DNS funciona um pouco como as nossas agendas telefónicas, que nos permitem seleccionar o nome de uma pessoa e ligar-lhe sem termos de conhecer de memória o seu número de telefone.

A especificação inicial do DNS não contempla quaisquer políticas ou mecanismos de segurança para evitar ataques à resolução de nomes. O seu desenho consiste fundamentalmente e dá primazia a aspetos de eficácia, eficiência e escalabilidade. Por este facto, a especificação possui diversas vulnerabilidades de segurança, que têm vindo a ser exploradas ao longo dos anos.

O DNSSEC surgiu para assegurar a correta comunicação entre diferentes sistemas informáticos, procurando minimizar alguns riscos da navegação na Internet. Essa extensão tem por base a utilização de tecnologia de criptografia assimétrica, que assegura a autenticidade e a integridade da informação trocada entre servidores DNS e entre estes e as aplicações do utilizador.

A autenticidade e integridade da informação trocada entre servidores DNS reduz drasticamente a probabilidade de ataques tais como o *man-in-the-middle* ou a intercepção de comunicações - usados em esquemas de roubo de identidade e fraude bancária-, o que resulta numa internet mais segura para os utilizadores.

Vários países definiram já como obrigatório o uso desta tecnologia nos nomes internet dos sistemas informáticos do Estado e da Administração Pública. Em Portugal a adopção desta tecnologia tem sido muito lenta quer no sector público, quer no privado.

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

**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 Ingram Publishing

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