

Benefícios para empresas e clientes

O que é?

DNSSEC é um protocolo que está sendo implantado atualmente para proteger o sistema de nomes de domínio (DNS), o catálogo telefônico global da Internet. As pessoas preferem localizar servidores de Internet usando nomes (como icann.org), porém, nos bastidores, o DNS corresponde cada nome a um endereço numérico, para que os dados sejam transferidos para o dispositivo certo.

DNSSEC é a abreviação de Extensões de segurança de DNS ("DNS Security Extensions") O DNSSEC acrescenta segurança ao DNS incorporando criptografia de chave pública na hierarquia do DNS, resultando em uma infraestrutura de chave pública (PKI) única, aberta e global de nomes de domínio. Ele é o resultado de mais de uma década de desenvolvimento de padrões abertos da comunidade.

Quais são os benefícios do DNSSEC?

Uma pesquisa protegida com o DNSSEC é assinada digitalmente, protegendo-a contra modificações sub-reptícias e, portanto, contra ataques que podem, por exemplo, redirecionar um usuário final a um site impostor ou mal-intencionado para obter sua senha. Quando realizado por um ataque à infraestrutura de uma empresa ou de um provedor de serviços na Internet (ISP), todos os usuários da entidade são afetados. Isso geralmente é conhecido por envenenamento de cache. Proteção contra envenenamento de cache é um dos principais benefícios do DNSSEC.

No entanto, um dos maiores benefícios provavelmente surgirá

identidades, comunicações e programas, empresas e clientes pode em breve ser capaz de criar a expectativa de uma comunicação contínua e confiável em todas as fronteiras organizacionais e nacionais. Assinar os domínios raiz e de primeiro nível criou as condições para isso.

Como eu implemento o DNSSEC?

Para empresas:

Implantar o DNSSEC em infraestrutura de DNS corporativo ("ativar" a validação do DNSSEC)

Implantar o DNSSEC em seus nomes de domínio ("assinar" seus nomes de domínio corporativos)

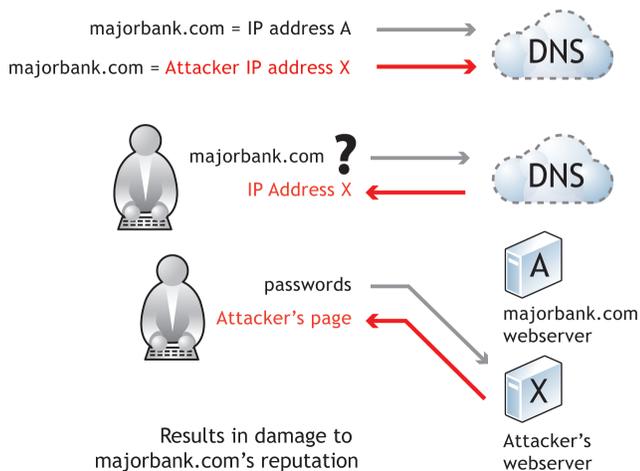
Para usuários:

Pergunte a seu ISP sobre o DNSSEC (obtenha validação "ativada" do DNSSEC em seus servidores de DNS)

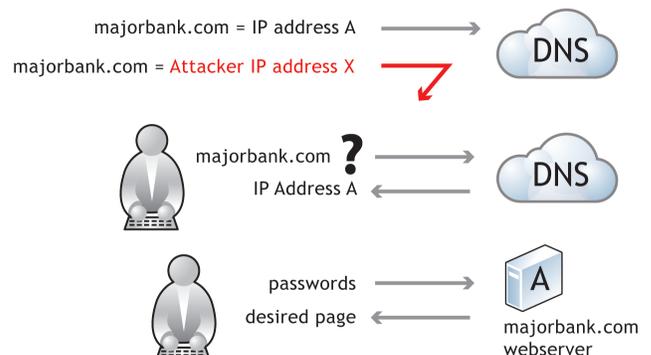
Papel da ICANN

- Gerenciar a chave raiz dessa hierarquia juntamente com o VeriSign (mediante contrato com o Departamento de Comércio dos EUA) e representantes internacionais confiáveis da comunidade da Internet.
- Processar solicitações de adições/alterações/exclusões de chave pública e outros registros em Registros na parte superior da hierarquia de DNS (i.e., .com, .se ...etc)
- Treinar e auxiliar a comunidade da Internet em relação ao DNSSEC

Without DNSSEC



With DNSSEC



Para orientação técnica:

- | | |
|------------------------------------|---|
| • IETF | http://www.ietf.org , http://tools.ietf.org/pdf/draft-ietf-dns-op-rfc4641bis-05.pdf |
| • DNSSEC Iniciativa de implantação | http://www.dnssec-deployment.org |
| • ISC | http://www.isc.org |
| • NLNETLABS | http://www.nlnetlabs.nl |
| • DNSSEC.NET | http://www.dnssec.net |

Grupos da comunidade ICANN envolvidos no DNSSEC:

- Commercial Stakeholders Group (CSG)
 - Commercial and Business Users Constituency (BC)
 - Internet Service providers and Connectivity Providers Constituency (ISPCP)
- Non-Commercial Stakeholders Group (NCSG)
 - Non-Commercial Users Constituency (NCUC)
- Security and Stability Advisory Committee (SSAC)

