DNSSEC sécurise Internet

Document accessible en ligne à l'adresse :
http://dnssec-deployment.icann.org/dnsseccard.pdf

ICANN
Un seul monde. Un seul Internet.
http://icann.org

Avantages pour les sociétés et les clients

Définition

DNSSEC désigne un protocole actuellement déployé pour sécuriser le système de nom de domaine (DNS), l'annuaire mondial d'Internet. Les hommes préfèrent localiser les serveurs Internet à l'aide de noms (comme icann.org) mais en réalité, le DNS fait correspondre chaque nom à une adresse chiffrée pour que les données soient transférées vers le bon appareil.

DNSSEC est l'abréviation de "DNS Security Extensions" (extensions de sécurité du DNS). DNSSEC ajoute un niveau de sécurité au DNS en incorporant une cryptographie de clé publique dans la hiérarchie du DNS, ce qui donne une seule infrastructure de clé publique (Public Key Infrastructure ou PKI), ouverte et mondiale pour les noms de domaine. C'est le résultat d'une dizaine d'années de développement aux standards ouverts auprès d'une communauté.

Quels sont les avantages de DNSSEC ?

Une recherche sécurisée avec DNSSEC possède une signature numérique qui la protège de toute modification subreptice et donc de toute attaque pouvant, par exemple, rediriger un utilisateur final vers un site fictif et malveillant ayant pour but la collecte de mots de passe. Si une entité se retrouve prise par une attaque sur une infrastructure de société ou de FAI, tous ses utilisateurs sont affectés. On parle souvent dans ces cas d'empoisonnement du cache (cache poisoning). La protection contre l'empoisonnement du cache est l'un des principaux avantages de DNSSEC.

Cependant, l'un des plus grands avantages est certainement sur le point d'émerger des efforts naissants pour utiliser la toute récente PKI mondiale pour sécuriser plus que les noms de domaine. En utilisant DNSSEC pour distribuer également des enregistrements (clés) et aider à sécuriser les e-mails, les sites Web, les identités, les communications et les programmes, sociétés et utilisateurs pourront bientôt prétendre à des communications fluides en toute confiance, sans se soucier de quelque frontière que ce soit. Ceci a été préparé par la signature des domaines racine et de premier niveau.

Comment mettre en place DNSSEC ?

Pour les sociétés :

Déployez DNSSEC sur l'infrastructure du DNS de la société (configurez la validation DNSSEC sur "on")

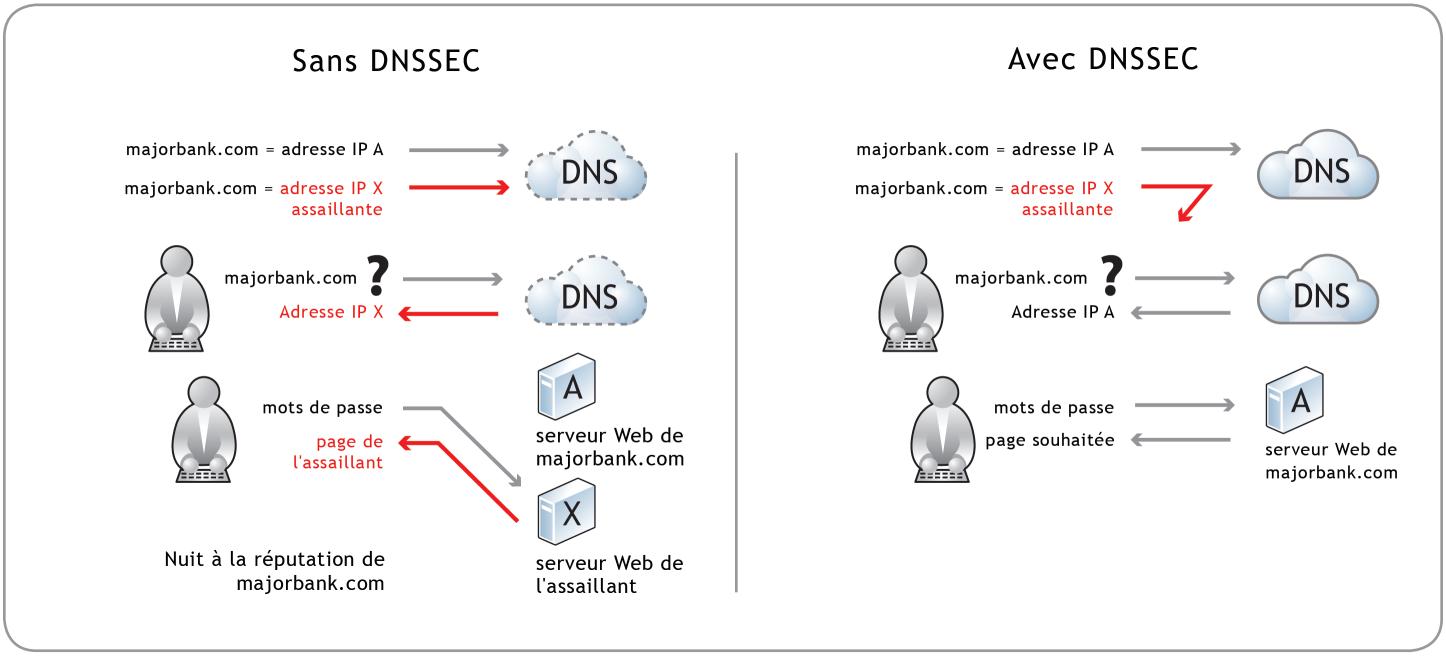
Déployez DNSSEC sur vos noms de domaine ("signez" vos noms de domaine d'entreprise)

Pour les utilisateurs :

Interrogez votre FAI sur DNSSEC (demandez à ce qu'il configure la validation DNSSEC sur "on" sur ses serveurs DNS)

Rôle de l'ICANN

- Gérer la clé racine de cette hiérarchie avec VeriSign (sous contrat avec le département du commerce des États-Unis) et des représentants de la communauté Internet internationaux et de confiance
- Traiter les demandes d'ajout/de modification/de suppression de clé publique et d'autres enregistrements des Registres au sommet de la hiérarchie du DNS (par exemple : .com, .se, etc.)
- Former et assister la communauté Internet à DNSSEC



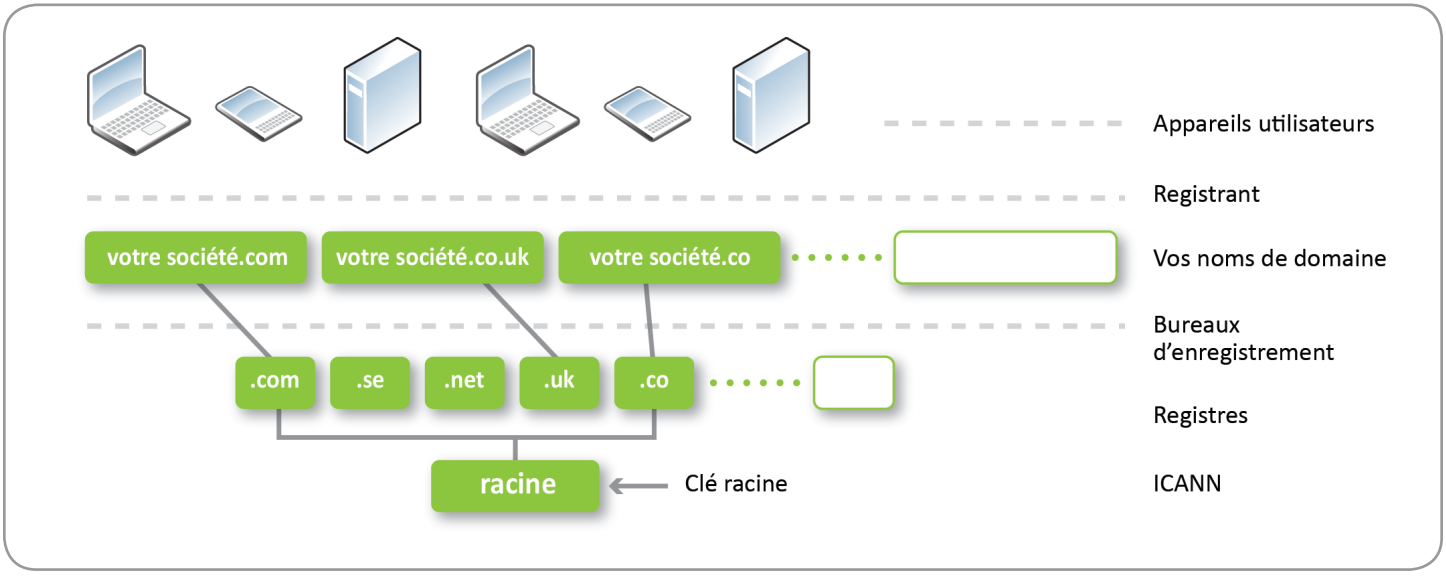
DNSSEC *sécurise Internet*

Pour tout conseil technique :

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

Groupes de communauté ICANN impliqués dans DNSSEC :

- Groupe de parties prenantes commerciales (Commercial Stakeholders Group ou CSG)
  - Collège regroupant les utilisateurs commerciaux et d'entreprise (BC)
  - Collège regroupant les Fournisseurs d'accès Internet et fournisseurs de connectivité (ISPCP)
- Groupe de parties prenantes non commerciales (NCSG)
  - Collège regroupant les utilisateurs non commerciaux (NCUC)
- Comité consultatif de stabilité et de sécurité (SSAC)



ICANN

Un seul monde. Un seul Internet.

http://icann.org