L'Afnic renforce la sécurité du «.fr»

Comment sécuriser davantage les transactions en ligne? L'une des réponses s'appelle **DNSSEC** (*Domain Name System Security Extensions*) que l'**Afnic** (Association française pour le nommage Internet en coopération) est en train de déployer dans la zone France (.fr) et Réunion (.re).

Cette nouvelle mesure de protection a été abordée suite à la découverte d'une faille dans le protocole DNS en 2008 par le chercheur en sécurité Dan Kaminsky. La vulnérabilité était susceptible de **faire tomber le Web** en menant une attaque par empoisonnement de cache. Une menace qui a mobilisé gouvernement et grands groupes à l'époque entraînant une prise de conscience sur la nécessité de déployer le protocole DNSSEC des acteurs de l'Internet (nommage, télécoms, hébergeurs…).

Un déploiement qui concerne en premier lieu les gestionnaires de serveurs DNS, les bureaux d'enregistrement et les FAI. Mais leur volontarisme est inégal, notamment en raison des coûts financiers inhérents. Ce qui est d'autant plus problématique que l'efficacité du protocole ne portera ses fruits qu'à travers une implication et une appropriation globale de tous les acteurs. *« Une attaque par empoisonnement de cache est toujours possible. On considère que 20 à 25% des serveurs dans le monde ne bénéficient pas d'une vraie mise à jour de sécurité »*, **Mathieu Weill**, directeur général de l'Afnic selon des propos cités par *ITespresso.fr*.

Rappelons que le DNSSEC n'est pas une nouveauté technique. L'**IETF** (Internet Engineering Task Force) l'a scruté dès 1995 et la Suède s'est montrée précurseur dans son adoption en 2007. Puis des pays comme la Bulgarie, le Brésil ou le Porto-Rico ont suivi… L'Afnic suit aujourd'hui le mouvement d'adoption devenu *«mainstream»*, selon Mathieu Weill. A ce jour, une quinzaine de registres ont déjà signé leurs zones… *« Toutes les extensions nationales devraient signer cette année »*, estime le directeur. La racine elle-même du DNS (gérée par l'ICANN et VeriSign) a été signée en juillet 2010. L'an prochain, ce sera au tour du plus générique des noms de domaine : «.com» (90 millions dans le domaine) alors que la conversion DNSSEC du «.org» a été effectuée en 2009.

Au tour, donc, de l'Afnic d'agir. Le 14 septembre dernier, le déploiement de DNSSEC en France a débuté avec la signature du «.fr» et du «.re». Prochainement, la clé publique de chiffrement associée au «.fr» sera publiée dans les serveurs racines. Ce qui bouclera la procédure technique. Mais, pour l'association de nommage, le plus gros effort reste à venir : **informer le grand public**, vulgariser, former les administrateurs de gestion DNS (FAI, hébergeurs, centres de bureau d'enregistrement…). *« Ce n'est pas obligatoire de déployer le DNSSEC mais nous estimons que c'est une responsabilité à chaque niveau »*, précise Mathieu Weill. Pour faciliter l'appréhension, l'organisme proposera bientôt la version 3 de ZoneCheck, son outil de test de configuration DNS (logiciel libre sous licence GPL et gratuit).

Quel sera le coût de déploiement de DNSSEC pour gestionnaire de DNS? *« Le budget sera variable. La fourchette de prix variera en fonction du degré de maîtrise escompté*, explique Mathieu Weill, *à l'Afnic, on ne fera pas payer une empreinte de clé dans notre système. »* Les bureaux d'enregistrement de noms de domaine pourront cependant répercuter le coût de mise à jour sur la facture de leurs clients.