DNSSEC

Sécurisation de vos noms de domaine

Lorsque vous vous connectez à un site web et que vous saisissez des informations personnelles, comment pouvez-vous avoir la certitude que vos informations sont sécurisées ? L'utilisation du protocole DNSSEC peut vous y aider.

Le protocole DNSSEC agit comme un système de protection inviolable des données de noms de domaine, vous assurant de communiquer avec un site web ou un service qui n'a pas été falsifié.

La validation DNSSEC finira par être intégrée aux systèmes d'exploitation et sera un élément fondamental de l'infrastructure réseau.

Peu de technologies sont aussi cruciales pour le fonctionnement de l'Internet que le système de noms de domaine (DNS, Domain Name System). Les extensions de sécurité DNS - communément appelées DNSSEC - permettent aux utilisateurs d'accroître leur confiance dans les activités en ligne qui font de plus en plus partie de notre mode de vie : sur le lieu de travail, à la maison et à l'école. Le protocole DNSSEC agit comme un système de protection inviolable des données de noms de domaine, vous assurant de communiquer avec un site web ou un service qui n'a pas été falsifié.

Qu'est-ce que le protocole DNSSEC ?

Avant de vous connecter à un site web, votre navigateur utilisera le DNS pour récupérer une adresse IP pour le site que vous avez choisi. Néanmoins, une personne malveillante peut intercepter votre requête DNS et fournir de fausses informations qui vous dirigeront vers un faux site web où vous pourriez éventuellement fournir des renseignements personnels (par exemple, un site qui vous semble être celui d'une banque). Le protocole DNSSEC vous garantit d'obtenir exactement les informations publiées par le propriétaire du nom de domaine.

Le protocole DNSSEC fournit un niveau de sécurité supplémentaire afin que votre navigateur puisse veiller à ce que les informations du DNS n'ont pas été modifiées. Il ne traite pas toutes les menaces (nul n'y parvient), mais fournit un bloc de construction pour assurer une sécurité supplémentaire des données, non seulement dans le DNS, mais aussi dans les applications et les services qui reposent dessus. Le DNSSEC permet par exemple l'utilisation du protocole DANE qui peut augmenter le niveau de confiance et de sécurité des certificats TLS/SSL pour le commerce électronique et l'accès sécurisé aux sites et aux services.

Notez aussi que le DNSSEC n'est PAS uniquement destiné au Web, mais qu'il peut être utilisé par un autre service ou protocole Internet. Il existe déjà des utilisations intéressantes du DNSSEC avec les applications d'e-mail (SMTP), de messagerie instantanée (IM) et de voix sur IP (VoIP).

Internet Society

www.internetsociety.org

À propos de l'Internet Society.

L'Internet Society est une source d'informations et de leadership indépendante et fiable sur les questions liées à l'Internet. Grâce à sa vision, à ses principes et à ses fondements technologiques importants, l'Internet Society encourage un dialogue ouvert sur les questions politiques et technologiques liées à l'Internet et œuvre en faveur de son développement futur parmi les utilisateurs particuliers et au sein des entreprises, des gouvernements et d'autres organisations. En travaillant avec ses membres et ses chapitres du monde entier, l'Internet Society favorise l'évolution et la croissance continues de l'Internet pour tous.

Apportez votre contribution : déployez le DNSSEC sur votre(vos) nom(s) de domaine.

La signature de votre domaine avec DNSSEC comporte deux volets :

1. Le bureau d'enregistrement de votre nom de domaine doit être en mesure d'accepter les enregistrements DS (Delegation Signer) et les envoyer au domaine de premier niveau (TLD, Top Level Domain) (comme .com, .org, ou .net).
2. Le fournisseur d'hébergement DNS qui gère les serveurs de noms DNS pour votre domaine doit prendre en charge le DNSSEC et être en mesure de signer (et re-signer) vos fichiers de zone DNS.

Certains bureaux d'enregistrement peuvent remplir les deux rôles pour vous. Parfois, les enregistrements DNS de votre domaine peuvent être hébergés par un autre fournisseur, ou vous pouvez les héberger vous-même sur vos propres serveurs DNS.

Apportez votre contribution : utilisez le DNSSEC.

En tant qu'utilisateur final, vous avez plusieurs options pour vous assurer que vous utilisez le DNSSEC :

- Votre résolveur DNS local (depuis votre fournisseur d'accès à Internet (FAI) ou votre réseau local) peut effectuer la « validation DNSSEC » et bloquer automatiquement les sites avec des signatures DNSSEC incorrectes.
- Vous pouvez également installer un résolveur DNS de validation sur votre ordinateur local.
- Vous pouvez ajouter le support de DNSSEC directement dans un navigateur web.

La validation DNSSEC finira par être intégrée dans les systèmes d'exploitation et sera un élément fondamental de l'infrastructure réseau ; mais avant cela, il y a des mesures que vous pouvez prendre si vous êtes techniquement performant et intéressé par la sécurité.

Demandez de l'aide.

Le programme Deploy360 de l'Internet Society fournit des ressources pour le déploiement effectif de l'IPV6 et DNSSEC. Deploy360 comble le fossé entre le processus de normalisation de l'IETF et l'adoption finale de ces normes par la communauté mondiale chargée des opérations. Deploy360 crée et fournit des ressources qui sont faciles à comprendre et qui peuvent être rapidement mises en action par les professionnels des TI chargés de la mise en œuvre de nouvelles technologies et normes telles que l'IPv6 et le DNSSEC.

Consultez le site www.internetsociety.org/deploy360/dnssec pour en savoir plus et consultez la page de notions élémentaires et les projets spécifiques pour vous aider à démarrer avec DNSSEC.