EXTENSIONS DE SÉCURITÉ DU SYSTÈME DES NOMS DE DOMAINE

CONTRIBUEZ À SÉCURISER LES INFORMATIONS DNS QUE VOUS ENVOYEZ SUR INTERNET

Les extensions de sécurité du système des noms de domaine (DNSSEC) permettent aux titulaires de noms de domaine de **signer numériquement** l'information qu'ils envoient à travers le système des noms de domaine (DNS). Il s'agit d'un moyen de protéger les consommateurs en évitant qu'ils reçoivent des données DNS ayant été corrompues de manière accidentelle ou illicite.

CHRONOLOGIE

1980

Au moment de la création du DNS, la sécurité n'était pas au cœur de sa conception. Les attaquants pouvaient **compromettre vos messages DNS et les rediriger ailleurs** sur Internet au lieu de les délivrer à leurs destinataires

1990

La communauté technique du DNS crée la solution définitive à ce problème : les DNSSEC. Les DNSSEC renforcent l'authentification dans le DNS à l'aide de signatures numériques basées sur une **cryptographie à clé publique.**

LES DNSSEC À L'OEUVRE

Les deux côtés des DNSSEC doivent être activés pour que les extensions de sécurité fonctionnent.

Les titulaires de noms, qui sont responsables de la publication des informations sur le DNS, doivent **s'assurer que leurs données DNS sont signées DNSSEC.**

Les opérateurs de réseau doivent **activer la validation DNSSEC dans les résolveurs** qui gèrent les recherches DNS pour leurs utilisateurs.

AVANTAGES DU DÉPLOIEMENT DES DNSSEC

Protection de l'Internet, des utilisateurs finaux, des entreprises, des organisations et des gouvernements.

Réduction de la vulnérabilité aux attaques.

Promotion de l'innovation. Les DNSSEC vérifient et protègent les données DNS, qui deviennent donc fiables pour des applications au-delà du DNS.

ENCOURAGEZ VOS OPÉRATEURS DE RÉSEAU À ACTIVER LES DNSSEC

ICANN

POUR DE PLUS AMPLES INFORMATIONS SUR LES DNSSEC, RENDEZ-VOUS SUR :

http://go.icann.org/OCTOpublications
http://go.icann.org/DNSSEC

Conçu par le département de la communication de l'ICANN | Mai 2020