Un guide du NIST pour sécuriser les serveurs DNS

Publié le vendredi 26 mai 2006
Voir en ligne : https://www.france-science.org/Un-guide-du-NIST-pour-securiser.html

Le NIST a publié un guide, " Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide " de déploiement de serveurs de noms de domaines (DNS) sûrs destinés aux entreprises, sponsorisé par le Department of Homeland Security. Constatant que les DNS sont souvent la cible d'attaques visant soit à corrompre les données, soit à interrompre l'accès à celles-ci par déni de service (DoS), le guide propose des recommandations génériques (pour éviter la compromission de serveurs) et spécifiques aux DNS. En particulier, il recommande l'utilisation de méthodes cryptographiques (codes d'authentification de message et signatures numériques) pour assurer l'intégrité et l'authenticité des données transmises lors des mises à jour, réplication de données et transactions réquête/réponse. L'absence de ces fonctions facilitait les attaques visant à compromettre l'intégrité des données. Le guide s'appuie sur la spécification DNSSEC (Domain Name System Security Extentions) de l'IETF.

Source :

http://www.fcw.com/article94546-05-17-06-Web&newsletter%3Dyes

Pour en savoir plus, contacts :

Secure Domain Name System (DNS) Deployment Guide
http://csrc.nist.gov/publications/nistpubs/800-81/SP800-81.pdf
Code brève
ADIT : 33789

Rédacteur :

Sébastien Morbieu, deputy-stic.mst@ambafrance-us.org