Dan Kaminsky recommande un patch global et permanent contre la faille DNS

Celui qui se fait désormais surnommer le père de la faille DNS met en garde. Durant le ***Black Hat***, raout des pirates et autres professionnels de la sécurité, il a donné **quelques–uns de ses derniers conseils.**

Expert au sein de l'équipe d **'IO Active**, il a recommandé aux professionnels de la sécurité de prendre des mesures en faveur d'une **prise en compte générale de la sécurité des réseaux**. En cause, la technologie de défense **DNSSEC**. Ce protocole qui permet de protéger certains réseaux devrait, selon Kaminsky être généralisé de manière permanente car il offre une meilleure méthode d'**authentification et de protection des données** contre les attaques d'empoisonnement du cache (***cache poisonning***).

Une technologie largement soutenue par le gouvernement fédéral des Etats-Unis pour ses propres réseaux. Cependant, de n **ombreuses entreprises rechignent encore à déployer des solutions** utilisant la technologie DNSSEC (selon Kaminsky) à cause de sa complexité.

L'expert commente : « *La technologie* ***DNSSEC peut apparaître terrifiante lorsque l'on doit l'implémenter****. Il y a tellement d'administrateurs qui sont censés le faire mais peu ont encore essayé*« .

Dan Kaminsky a tenu à expliquer que les failles était inhérentes au DNS et qu'il était du ressort des industriels de la sécurité de se saisir de la question afin de généraliser les process. « *Une fois que les systèmes sont implémentés, les administrateurs n'ont seulement plus qu'à****défendre leurs serveurs DNS contre les attaques du cache****. C'est tout* « .

Si le système de patch a contribué à protéger les systèmes et domaines les plus utilisés, Kaminsky constate que certains services ou réseaux subalternes sont toujours exposés. Il anticipe alors à un an le temps qu'il faudra pour protéger tous les réseaux majeurs. Le site*Computerworld* estime **à ce jour à 200.000 le nombre de serveurs DNS non-protégés contre la faille.**

Petit rappel, pour ceux qui sont partis en vacances (plusieurs mois…, loin de toute connexion Internet). En juillet dernier, ce défaut de taille dans la cuirasse du **DNS, le système central qui met en relation les adresses des sites et les pages stockées sur des serveurs** était découvert par le chercheur. Par cette découverte, tout le réseau mondial d'Internet a pris conscience du risque de voir des pirates s'emparer de l'ensemble du trafic. De fausses données DNS peuvent alors être insérées dans la cache d'un name-server. Un attaquant peut alors afficher une mauvaise réponse pour n'importe quelle requête et rediriger un internaute vers un site piégé à son insu.

Une riposte sous forme de correctif était alors arrivée par des **mises à jour proposées par Microsoft** et les éditeurs de sécurité puisque la vulnérabilité du **protocole DNS** affectait aussi bien les serveurs de cache déployés par les fournisseurs d'accès à Internet que les postes clients utilisés par les internautes.

Par ce commentaire, l'expert confirme une étude menée en septembre dernier. Selon **NBS System**, société spécialisée dans la sécurité informatique, près de **33% des DNS français étaient encore**

sensibles à cette faille. Et à ce jour ?