DNS : les attaques augmentent et la facture s'alourdit

Usurpation, empoisonnement du cache DNS (Domain Name System), déni de service distribué (DDoS), réflexion avec amplification… Les attaques DNS se multiplient.

C'est ce qui ressort du « Global DNS Threat Report 2019 » publié par EfficientIP, en partenariat avec IDC. Les responsables IT de 904 organisations ont été interrogés.

82% des entreprises concernées par l'enquête* ont été la cible d'attaques DNS en 2018. Un chiffre en hausse de 5 points par rapport à l'édition précédente du rapport.

En moyenne, elles ont été la cible de 9,45 attaques DNS par organisation en 2018, contre 7 l'année précédente.

Ces attaques ont le plus souvent entraîné un arrêt d'applications internes (dans 63% des cas d'attaques DNS) et/ou la compromission de sites Web (45%).

La facture globale s'en ressent.

Ainsi, le coût moyen par attaque DNS (restauration de services et perte de chiffre d'affaires) a augmenté de 49% pour atteindre 1,27 million de dollars (1,16 M€) toutes régions étudiées confondues.

En France, la hausse est moins marquée, mais elle a été de +8% toute de même à 940 000 euros, selon le rapport.

Globalement, la finance est la plus ciblée (88% des organisations du secteur ont subi des attaques DNS). L'éducation, de son côté, est le secteur le plus exposé au phishing.

Zero Trust, la clé d'une sécurité réseau renforcée ?

Une minorité (38%) considère la protection de leur DNS comme une priorité.

« Lorsqu'elles sont attaquées, les entreprises ne peuvent pas arrêter toute leur activité, mais elles peuvent contenir le risque », a déclaré dans les colonnes de *DarkReading* Ronan David, VP développement d'affaires et marketing d'EfficientIP.

Pour le fournisseur franco-américain de solutions de sécurisation et automatisation réseau, « maintenir le service, la disponibilité, la bande passante et le contrôle – autant d'éléments essentiels à l'intégrité du réseau – est indispensable. La reprise après sinistre et l'évitement de points uniques de défaillance doivent faire partie du processus d'atténuation. Pour ce faire, il est essentiel d'adopter une stratégie 'zero trust' (confiance zéro). »

**L'enquête a été menée à la demande d'EfficientIP par IDC de janvier à avril 2019 auprès de 904 professionnels de l'IT, parmi lesquels des DSI et des RSSI. Trois régions sont couvertes : Amérique du Nord, Europe et Asie-Pacifique.*

(crédit photo © nikkytok – shutterstock)