Ransomwares : les entreprises françaises touchées, se distinguent

SentinelOne, spécialiste de la sécurité, a commandé une étude à Vanson Bourne sur les ransomwares. Interrogeant 500 entreprises dans plusieurs pays, dont 100 en France, le cabinet d'études livre un rapport riche en renseignements. Le premier est que le rançongiciel est plus qu'un buzzword. C'est devenu une réalité dramatique pour beaucoup d'entreprises. 48% des sociétés admettent avoir subi une attaque au cours des 12 derniers mois. La France se démarque un peu en prenant la tête des pays les plus touchés (52%). Dans l'hexagone, 60% des sondés ont dû faire face entre 1 et 4 attaques par an.

Le vecteur d'attaques des rançongiciels reste pour une majorité d'organisations (81%) le phishing via la messagerie. La France tire son épingle du jeu avec « seulement » 69% des entreprises touchées via l'hameçonnage. Elle est par contre plus visée par les infections à travers des botnets (46%) que ses homologues anglais (18%). Les informations les plus ciblées au global sont les données des salariés (42%). Mais en France le tiercé de tête se focalise sur les données métiers (clients, finance et produits).

Une réparation chronophage

Différences aussi sur le succès des attaques. Pour plus de la moitié des entreprises françaises (52%), les attaquants ont été capables de chiffrer les données et les fichiers, mais elles ont été à même de les déchiffrer. Elles sont 27% à avoir fait le deuil et fait appel à leur solution de sauvegarde. Une tâche qui mobilise du temps et des moyens humains. L'étude évalue en moyenne à 38 heures-hommes en France pour remplacer les données chiffrées par celles du back-up. Au niveau mondial, cet indicateur s'établit à 33 heures-hommes.

Autre impact collatéral des ransomwares, ils bouleversent la perception et la mise en œuvre des politiques de sécurité. 67% des sondés augmentent leurs dépenses en matière de sécurité pour éviter une récidive. Plus de la moitié (53%) ont modifié leur stratégie pour s'orienter vers la remédiation. Une certaine méfiance s'installe vis-à-vis des solutions de sécurité dans leur capacité à bloquer les ransomwares.

Les allemands prêts à virer RSSI et DSI

Les allemands sont encore plus lapidaires avec 25% des entreprises prêtes à couper les têtes des RSSI et des DSI, surtout dans le secteur du bâtiment (47%) et le secteur public (31%). On notera en France une plus grande sensibilité au risque d'avoir mauvaise presse et une mauvaise publicité suite aux attaques.

Autre distinction, les entreprises nationales françaises (52%) comme allemandes (53%) demandent à leur division IT de notifier leurs incidents en priorité aux régulateurs en charge de la protection des données, plutôt qu'à la direction. Les anglo-saxons sont plus procéduriers et en réfèrent

directement auprès des avocats, après en avoir informé les dirigeants et le conseil d'administration de la société.

A lire aussi :

Ransomware : les entreprises françaises passent à la caisse

Le ransomware Cerber chasse les bases de données des entreprises

Crédit Photo : LeoWolfert-Shutterstock