Ransomware : les entreprises françaises passent à la caisse

L'année 2016 aura été sans conteste celle des ransomwares. Pas une étude sur la cybersécurité qui ne place ce phénomène en tête des menaces pour les entreprises. Des hôpitaux aux écoles, en passant par les PME et les grands comptes, personne n'échappe à ce risque. Et les organisations françaises ne sont pas à l'abri bien au contraire.

Dans une étude menée par Trend Micro, les DSI interrogés ont globalement (64%) une connaissance des rançongiciels (fonctionnement et mode opératoire). Seulement 16% avouent n'en avoir jamais entendu parler. Un point important à souligner est la résignation face à la menace. En effet, 60% des sondés estiment que leur organisation sera infectée par un ransomware dans les 12 prochains mois. Une renonciation assumée, 91% des DSI estiment le danger réel et sont conscients du préjudice que ces malwares peuvent causer.

La moitié des DSI paye la rançon

Sur les attaques, ils sont 40% à avouer avoir été touchés dans les deux dernières années. Et le plus inquiétant est la réponse apportée par les entreprises à ces attaques. 50% des décideurs IT acceptent de payer la rançon. Pourquoi ? Trend Micro leur a demandé les raisons et 3 réponses sortent du lot. Il y a tout d'abord la problématique de la réputation en cas de disparition des données (40%). En second lieu, le montant de la rançon est suffisamment bas pour être absorbés dans les coûts d'exploitation (40% aussi). Enfin, le besoin de reprendre rapidement la main sur les données est cité dans 32% des cas.

Pour autant, si les entreprises payent, elles ne sont que 32% à récupérer effectivement leurs données. Loïc Guezo, stratégiste cybersécurité pour l'Europe du Sud chez Trend Micro, rappelle : « *Le mot d'ordre en cas d'infection est de ne pas payer. Il est crucial de prendre conscience que nous avons avant tout à faire à des criminels à qui il ne faut jamais faire confiance.* » A noter que 70% des entreprises infectées ont reçu de l'aide des autorités et que cela a été bénéfique dans 40% des cas.

Sauvegardes et sensibilisation

L'éditeur japonais de sécurité rappelle certaines statistiques concernant les ransomwares. La rançon moyenne est de 638 euros et un quart des répondants avouent avoir été sollicités pour un montant supérieur à 1000 euros. Le délai moyen imparti pour payer la rançon est de 21 heures.

Autre chiffre à mettre en perspective, 29 heures en moyenne sont nécessaires pour réparer une infection par ransomware. Trend Micro rappelle que la mise en place de sauvegardes reste la façon la plus sûre de se prémunir contre ce danger. Et la majorité des entreprises (96%) possèdent une sauvegarde et une récupération automatique des fichiers critiques.

La sensibilisation des collaborateurs aux risques des rançongiciels est importante. Elle peut se faire à travers un programme de prévention. 70% des DSI en ont développé un et 26% prévoient d'en

développer un dans le futur. Un écho au guide de l'hygiène informatique de l'ANSSI…

A lire aussi :

Ransomwares : ingéniosité, perversité et persévérance

No More Ransom : coordination européenne contre les ransomwares

Crédit Photo : Bacho-Shutterstock