WannaCry et NotPetya laissent-ils les DSI de glace ?

L'ISACA, une association regroupant des professionnels de l'audit, de la sécurité et de la gestion des risques, a mené une étude originale auprès des responsables IT à la suite des attaques WannaCry et NotPetya. 450 DSI étaient interrogés sur les réponses apportées après ces différentes offensives.

Au regard des résultats, les DSI ne semblent pas pressés pour installer les dernières mises à jour publiées par Microsoft pour son OS Windows, y compris XP. Ainsi, ils sont moins de 25% à installer les mises à jour dans les premières 24 heures suivant l'attaque. D'autres n'hésitent pas à attendre plus d'un mois pour le faire. Les avocats des DSI plaideront que mettre à jour des équipements relève du parcours du combattant et peut s'avérer long et risqué surtout quand on touche à la production.

Un système de patching rapide et complet

Matt Loeb, CEO d'ISACA, s'émeut de ce fort taux de responsables IT effectuant des mises à jour à retardement. « *Compte tenu de l'élévation et de la complexité des menaces auxquelles les entreprises sont confrontées, la mise en place d'une procédure de patching rapide est une composante essentielle de la sécurité d'une entreprise face aux conséquences d'une attaque contre l'organisation et ses infrastructures.* »

Malgré les expériences récentes, rien n'y fait pour 15% des DSI qui indiquent ne pas avoir pris des mesures spécifiques pour éviter ces menaces. Un décalage avec une prise de conscience du risque, 83% des DSI savent qu'ils vont avoir à faire face à des attaques par ransomware dans un proche avenir. Pour 6% des sondés, ils sont même prêts à payer la rançon. On pourra se rassurer en pensant que 50% des responsables IT ont mis en place des programmes de formation auprès du personnel pour savoir comment réagir. Il n'en demeure pas moins que 76% des répondants avouent que leur entreprise n'est pas bien préparée face à la fréquence des ransomwares.

A lire aussi :

Le plus grand risque de sécurité pour les DSI ? Les PDG !

Quand un DSI laisse des backdoors pour pirater son ancien employeur

Photo via Visualhunt.com