Lutte anti-ransomware : les entreprises françaises privilégient la sensibilisation

Malwarebytes s'est intéressé à l'approche des PME et ETI françaises pour se protéger des ransomware.

Les logiciels rançonneurs ont particulièrement été actifs sur la première moitié de l'année avec des attaques à l'échelle mondiale qui ont touché des entreprises comme Saint-Gobain, Renault, Maersk ou Honda victimes de malware comme WannaCry, NotPetya, Petya et autre Locky. Un fléau qui touche aussi des hôtels, hôpitaux, établissements scolaires…

Le fournisseur de solutions de sécurité IT a interrogé les responsables cybersécurité de 175 entreprises françaises de moins de 1000 salariés courant juin. Des enquêtes similaires ont été menées aux USA, au Royaume-Uni, en Allemagne, en Australie et à Singapour.

Premier enseignement : les PME et ETI françaises sont bien au fait de l'existence du problème. Elles sont 88% à considérer le problème des rançongiciels comme une priorité. Une prise de conscience supérieure à la moyenne mondiale (75%).

Mais seules 11% des organisations du territoire national considèrent pertinente l'approche technologique pour lutter efficacement contre les ransomware. Contre 39% dans les autres pays (toujours en moyenne).

Formations à l'appui

Une vision pleine de bon sens puisque les malwares rançonneurs se propagent, à la source, par l'installation d'un fichier malveillant, généralement fourni en pièce jointe d'un e-mail frauduleux. Si ce fichier n'est pas activé, l'infection est évitée. D'où l'importance humaine dans la propagation des agents malveillants.

Ce n'est donc pas fortuit si 60% des organisations françaises considèrent la sensibilisation des personnes à la sécurité comme une solution pertinente de lutte contre les ransomware. Un sacré contraste avec les 30% constatés dans le reste du monde.

Cela se traduit par la mise en place de formation, plus ou moins continue, à la sécurité par 43% des entreprises sondées en France. Soit 2,5 fois plus que la moyenne mondiale (16%). Et 81% assurent au moins deux cessions de sensibilisation par an. Contre 47% seulement des entreprises dans le monde. Néanmoins, 10% des organisations françaises n'ont rien entrepris pour lutter contre les Locky et compagnie.

La sauvegarde des données privilégiée

Si les firmes nationales privilégient l'attention humaine pour éviter les infections, elles n'en négligent néanmoins pas les solutions technologiques. La sauvegarde des données est privilégiée

par 93% des sondées (69% dans le monde). Et 89% adoptent une solution de sécurisation de la messagerie. Un chiffre qui rejoint les 82% constatés hors de nos frontières.

La segmentation du réseau, qui limite la propagation des bestioles, est adoptée par plus de la moitié des organisations françaises. 37% choisissent de s'appuyer sur un prestataire de sécurité externe.

En cas d'infection et de prise d'otage des fichiers (par chiffrement), 67% des ETI et PME françaises refusent de payer pour récupérer leurs données (contre 59% ailleurs) même si les montant requis restent modestes (50% d'entre eux n'excèdent pas 1000 euros). Et une majorité de celles prêtes à ouvrir le porte-monnaie en bitcoins, n'acceptent de raquer que si les données rançonnées ont de la valeur.

Dans les faits, seules 25% des entreprises ayant refusé de payer ont perdu des fichiers. Contre 32% en moyenne mondiale. *« Il n'existe donc pas de corrélation entre la décision de payer et la perte de fichiers »*, conclut Malwarebytes. Sans parler de celles qui ont payé et n'ont pas récupéré leurs informations.

Lire également
La France, 4eme pays le plus touché au monde par WannaCry
Ransomwares : 38 % des victimes paient leur rançon
Le nouveau Locky vise les entreprises françaises