Etude Gigamon : État et progression des ransomwares en France

Internet

Posté par : JPilo

Publié le : 30/9/2022 14:00:00

Ce n'est plus un secret mais ces dernières années, les entreprises se sont retrouvées assaillies de toute part face à l'augmentation significative des attaques par ransomwares.

En effet, les ransomwares ont pris une telle place dans le paysage cyber que les équipes de sécurité du monde entier doivent constamment redoubler d'effort afin d'adapter leurs pratiques et leurs processus face à cet environnement cyber en constante évolution.

Pour comprendre l'ampleur de ce phénomène, Gigamon, l'expert de l'observabilité avancée, a mené une étude mondiale sur l'état et la progression des ransomwares et du paysage des menaces.

Il en ressort notamment que 95% des DSSI/RSSI déclarent avoir subi des attaques par ransomware au cours de l'année écoulée.

Un paysage hostile

La pandémie mondiale a bouleversé les entreprises du secteur de l'IT qui ont dû opérer une véritable métamorphose dans un laps de temps très court pour s'adapter au nouveau contexte et rester résilientes.

Cela a ainsi donné naissance à de nombreux projets de transformation numérique accélérés pour accompagner le passage au cloud. Une situation dont les cybercriminels ont su tirer profit pour multiplier leurs attaques par ransomwares et dérober des données aux entreprises.

Aujourd'hui, à mesure que nous entrons dans une ère post-pandémie, la situation ne semble guère s'améliorer pour autant. En effet, 56% des DSI/RSSI français reconnaissent que la crise des ransomwares est aggravée au cours des trois derniers mois.

Fort heureusement, les conseils d'administrations des entreprises françaises sont conscients de l'ampleur du risque ransomware et considèrent cette menace comme une préoccupation prioritaire (86%).

Sur la question des méthodes d'attaque par ransomware observées en France au cours de l'année écoulée, les personnes interrogées citent en premier lieu le phishing (56%) et les virus informatiques comme les logiciels malveillants (56%). Dans un second temps viennent, le smishing (phishing par SMS) (31%), les menaces internes accidentelles (30%) et les applications cloud (28%).

Une recrudescence d'attaques ransomwares aux causes multiples

L'enquête a également interrogé les professionnels de la sécurité français sur ce qu'ils considèrent être comme les principaux facteurs et causes de l'augmentation de la fréquence des attaques par ransomware. Pour 63% d'entre eux, l'aggravation de la crise est principalement due à la sophistication croissante des cybercriminels. Parmi les autres causes, les professionnels citent :

â€¢ La complexité croissante des environnements hybrides et multicloud qui crée de nouvelles vulnérabilités que les solutions traditionnelles ne peuvent pas détecter (40 %)

â€¢ La pénurie de compétences IT (40 %)

â€¢ La menace interne (29%)

Pour lutter contre cette menace qui ne laisse aucun répit aux équipes de sécurité, le besoin d'une plus grande visibilité pour identifier les endroits où¹ les ransomwares peuvent se cacher est désormais indispensable.

L'observabilité comme moyen de défense

Dans un contexte de ressources moindres, de plus grande complexité liée aux environnements hybrides et d'une mauvaise configuration du cloud, la visibilité est un des leviers principaux de l'atténuation du risque de ransomware. En effet, sans une vision plus globale et précise, il devient compliqué pour les entreprises d'anticiper et gérer les attaques les plus sophistiquées.

Pour les prochains mois, les entreprises françaises envisagent de concentrer leurs efforts sur :

â€¢ La sensibilisation et formation à la sécurité pour tous les collaborateurs compte tenu du nouveau modèle de travail hybride : 89%

â€¢ L'adoption d'une architecture de Zero Trust pour encourager une culture de la sécurité axée sur la vérification et la confiance implicite : 57%

â€¢ Permettre l'observabilité avancée, une visibilité holistique, sur l'ensemble de l'infrastructure IT 50%

Si l'investissement dans un plus grand nombre d'outils est en général une des premières solutions identifiées, les entreprises ont pris conscience qu'elles ne peuvent plus continuer à les empiler pour résoudre leurs problèmes de sécurité.

D'après l'étude Gigamon, 57 % des professionnels interrogés reconnaissent que les outils de sécurité qu'ils utilisent actuellement ne sont pas si efficaces sans une visibilité complète. Raison pour laquelle, il est indispensable d'opter pour une optimisation de la visibilité.

L'observabilité avancée est de plus en plus synonyme de protection contre les ransomwares, en particulier dans le cloud. L'enquête révèle notamment que 85% des responsables français de la sécurité interrogés affirment que l'observabilité avancée est un élément important de la sécurité du cloud.

Méthodologie :

Gigamon a analysé les témoignages de 1020 décideurs IT et sécurité sur six marchés mondiaux clés : les États-Unis, le Royaume-Uni, la France (200), l'Allemagne, l'Australie et Singapour.