Cyberattaque NotPetya : 5 ans aprÃ¨s : quelles leÃ§ons en tirer ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 6/7/2022 13:00:00

La semaine derniÃ¨re a marquÃ© le cinquiÃ¨me anniversaire des cyberattaques NotPetya, qui ont entraÃ®nÃ© des consÃ©quences destructrices dans le monde entier.

Dans ce contexte, je vous propose le commentaire de Regis Alix, Senior Principal Solutions Architect de Quest Software - fournisseur mondial de logiciels de gestion des systÃ¨mes et de sÃ©curitÃ©

"NotPetya est connue comme l'une des cyberattaques les plus destructrices de notre histoire. Elle aura coÃ»tÃ© Ã elle seule plus de 10 milliards de dollars en 2017 et s'est rÃ©pandue dans le monde entier pour infecter des milliers de machines en moins de 3 heures.

Contrairement Ã son prÃ©dÃ©cesseur, le malware Petya, NotPetya avait pour objectif de dÃ©truire et non de rÃ©clamer une ranÃ§on. Les malfaiteurs ont altÃ©rÃ© la clÃ© (sur l'Ã©cran de notification du ransomware) pour la rendre invalide.

L'attaque a mis de nombreuses entreprises face Ã leurs lacunes et a montrÃ© que les malwares ne respectent ni rÃ¨gles, ni frontiÃ¨res, ni les limites des structures IT. Chaque organisation pourrait tout simplement subir des dommages collatÃ©raux lorsqu'un partenaire commercial est attaquÃ©.

Le gÃ©ant du transport maritime Maersk fut parmi les entreprises les plus impactÃ©es : 45 000 ordinateurs ont Ã©tÃ© chiffrÃ©s, y compris tous les contrÃ´leurs de domaine Active Directory, sauf un. Ce qui leur fut salutaire, comme l'a dit un membre de l'Ã©quipe IT de Maersk : "Si nous ne pouvons pas restaurer nos contrÃ´leurs de domaine ... nous ne pouvons rien restaurer".

Maersk a appris que la restauration d'Active Directory n'est pas seulement critique, elle constitue un dÃ©fi unique en son genre. Les organisations doivent mettre en place un plan de restauration AD dÃ©diÃ©, pour relancer leur activitÃ© aussi rapidement et de maniÃ¨re aussi sÃ©curisÃ©e que possible.

Contrairement aux armes conventionnelles, les malwares peuvent Ãªtre rÃ©utilisÃ©s ou recyclÃ©s par l'ennemi. Les entreprises doivent par consÃ©quent anticiper le processus de restauration, en Ã©tablissant des prioritÃ©s, en planifiant et en effectuant des tests au moins une fois par an. D'autant plus qu'il est toujours possible que certaines vulnÃ©rabilitÃ©s ne puissent pas Ãªtre corrigÃ©es."