

# Simuler des attaques par ransomware pour entraîner ses équipes



© 2021 Les Echos Publishing

Les ransomwares sont des logiciels d'extorsion qui verrouillent l'ordinateur et demandent une rançon pour pouvoir, de nouveau, accéder aux données. Ils sont le plus souvent envoyés par email, via une pièce jointe vérolée ou un lien malveillant. Leur signalement a augmenté de 255 % entre 2019 et 2020, selon les chiffres de l'ANSSI (Agence nationale de la sécurité des systèmes d'information). C'est même devenu la cyberattaque la plus fréquente avec 60 % des attaques, selon le CERT-Wavestone. Dans 90 % des cas, les données finissent perdues, avec des conséquences irrémédiables pour les entreprises touchées. D'où l'importance de former ses collaborateurs à repérer les messages dangereux pour adopter les bons réflexes.

## Des solutions pour se tester

C'est ce que proposent plusieurs suites logiciels à travers des simulations d'attaques qui reprennent les techniques et les sujets habituellement utilisés par les cybercriminels. Elles permettent de tester les réactions des collaborateurs, d'apprendre à réagir et de faire prendre conscience des conséquences potentielles sur l'entreprise. L'ANSSI propose également un guide « Organiser un exercice de gestion de crise

cyber ». Ce document, téléchargeable gratuitement, vise à accompagner, pas à pas, les entreprises dans la mise en place d'un exercice de gestion de crise d'origine cyber vraisemblable et formateur.

Pour télécharger le guide :  
<https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/>

© 2021 Les Echos Publishing