Sensibiliser les utilisateurs, un moyen essentiel de lutter contre les ransomwares !

Une entreprise aura beau mettre en place le système de sécurité anti-ransomware le plus sophistiqué qui soit, il ne la protégera pas si les collaborateurs ne savent pas comment éviter les risques.

Temps de lecture : minute

2 mars 2022

Aucun système n'étant sûr à 100 %, les fournisseurs de services managés (MSP) n'ont d'autre choix que de traiter l'une des causes principales des failles de sécurité : les utilisateurs finaux. En les formant et les informant, vous pourriez à terme faire économiser des fortunes aux différentes parties impliquées.

Voyons de plus près comment se déroulent généralement les attaques de ransomwares, les moyens à disposition pour apprendre aux utilisateurs à les éviter, et les raisons pour lesquelles la prévention des ransomwares doit être prise au sérieux.

L'email : LA porte d'entrée des ransomwares

Des études ont montré que 92 % des malwares sont distribués via des emails. Les ransomwares, quant à eux, sont lancés pour la première fois depuis un email dans 40 à 90 % des cas. Clic sur un lien malveillant, téléchargement de pièce jointe semblant provenir d'une organisation légitime ou d'un collègue… L'email est la porte d'entrée par excellence des ransomwares. Au vu du nombre d'emails reçus chaque jour par un employé lambda, ce manque de vigilance n'a rien de surprenant.

Par ailleurs, l'email offre aux hackers un canal particulièrement adapté à l'établissement d'une relation avec les utilisateurs finaux, que cela passe par un scam ou par l'usurpation de l'identité d'un fournisseur avec lequel ils ont travaillé par le passé. Soyons honnêtes : qui ne suivrait pas à la lettre les instructions d'un message l'alertant que les informations de sa carte bancaire ont été compromises ou que son compte bancaire va être résilié ?

Aider les collaborateurs à reconnaître les signes d'une attaque

Pour minimiser le risque d'être victime d'un ransomware, une organisation doit s'assurer que ses salariés savent comment éviter de telles attaques. Même si investir d'investir dans la formation à la prévention des ransomwares, ne semble pas prioritaire, cette formation revient pourtant bien moins cher que le coût moyen d'une attaque, qui se monte en moyenne à près de 133 000 $. Pour aider les utilisateurs à mieux éviter les ransomwares, il faut leur montrer comment ces derniers se présentent, mais aussi l'impact de ces programmes malveillants sur leur entreprise et sur eux mêmes.

Une formation peut adopter les modalités suivantes :

- Sessions de formation à la cybersécurité obligatoires (une à deux fois par an)
- Campagnes continues de sensibilisation à la cybersécurité
- Formation des utilisateurs après un incident, à chaud

Une fois que les collaborateurs auront compris comment leurs actions peuvent avoir des conséquences sur eux, mais aussi sur ceux qui les entourent, ils se montreront plus vigilants.

Informer aujourd’hui pour économiser demain

Peu importe leur taille, toutes les organisations peuvent être victimes d’un ransomware. Mais les
conséquences de ces attaques ne se font sentir que longtemps après l’infection. La facture moyenne, en incluant les temps d’arrêt, les salaires, les coûts liés aux appareils et aux réseaux, les opportunités perdues et la rançon payée ? Les coûts associés à l’élaboration d’un programme de formation continue et à l’investissement dans des technologies anti-ransomware appropriées sont donc bien inférieurs aux répercussions financières d’une attaque par ransomware réussie.

Les entreprises devraient utiliser une solution qui s’appuie sur de véritables emails et pages Web de *phishing* interceptés. Lorsqu’un utilisateur interagit avec un email de phishing, l’outil en question alerte l’utilisateur et affiche un bref quiz interactif permettant d’évaluer son degré de sensibilisation au *phishing.* Ce mécanisme de formation très simple ne coûtera qu’une fraction des frais engendrés par une attaque de ransomware et se montrera redoutablement efficace.

La connaissance est clé

Le meilleur moyen d’aider les utilisateurs finaux à éviter les ransomwares consiste à les informer. L’être humain est très sensible aux stratégies de phishing et aux scams par email. Par ailleurs, il devient de plus en plus difficile de faire la différence entre du contenu frauduleux et du contenu légitime. Pourtant, il suffit de prendre le temps d’expliquer les bonnes pratiques de prévention des ransomwares, les tendances du " secteur " et les activités dont les collaborateurs doivent se méfier pour les empêcher de faire de graves erreurs.

C’est vrai, les simulations de ransomwares aident les utilisateurs à les reconnaître, mais sans contexte, les avantages de cette expérience ne sont pas optimaux.

Adrien Gendre, Chef Tech & Product Officer de Vade

Article écrit par Adrien Gendre