

Cyberattaque contre Ikea : Pourquoi encore les messageries ?

Internet

Posté par : JulieM

Publié le : 6/12/2021 13:00:00

L'enseigne Ikea a récemment confirmé être visée par des campagnes de phishing, et plus précisément de type « reply-chain ». Ses employés reçoivent en effet des emails qui semblent être des réponses à des messages envoyés précédemment. Il n'y en est rien, mais cette apparente légitimité incite les utilisateurs à les ouvrir, et à cliquer sur les liens qu'ils contiennent ou à en ouvrir les pièces jointes.

Pour Dirk Schrader, Global VP of Security Research chez Netwrix, ces attaques - qui compromettent l'infrastructure de messagerie interne - sont le cauchemar des équipes de sécurité :

« Les contrôles de sécurité en place ne sont généralement pas adaptés pour repérer ces attaques générant des emails envoyés depuis le domaine d'une entreprise. La majorité des employés ont en outre des difficultés à identifier ces emails malveillants.

Un expéditeur externe ou inconnu est en effet bien plus suspect, mais lorsque le message semble émaner d'un collègue, il est davantage probable que l'utilisateur clique sur un lien valide ou ouvre une pièce jointe malveillante. C'est pourquoi l'efficacité de cette méthode d'attaque est plus élevée que la moyenne.

L'objectif principal des cybercriminels est alors d'infiltrer autant d'appareils que possible pour mettre en place la première étape de l'attaque. La façon dont ces appareils seront ensuite utilisés dépend d'autres facteurs : leur protection, l'état des patches, et quel type de menace l'utilisateur a ouvert via un lien ou une pièce jointe.

Plus un attaquant dispose d'options, plus grandes sont ses chances d'atteindre l'objectif final, qui est de prendre le contrôle de l'infrastructure, d'exfiltrer des données ou de chiffrer des fichiers.

Pour se défendre, les entreprises peuvent utiliser les principes de sécurité de base préconisés par l'ANSSI, plus précisément en restreignant les privilèges et en utilisant un modèle ZeroTrust. La surveillance des points d'accès, pour détecter tout changement malveillant, représente une couche de sécurité clé qui devrait également être en place.

En effet, suite à la compromission initiale, les étapes suivantes d'une telle cyberattaque nécessiteront toujours pour poursuivre la campagne des téléchargements supplémentaires d'outils malveillants. Ces téléchargements et créations de fichiers doivent donc être détectés rapidement, d'autant qu'ils ne peuvent être corrigés à aucune activité habituelle des utilisateurs.

Dans l'ensemble, les entreprises doivent être conscientes de leurs données sensibles et des éléments critiques de leur infrastructure afin de savoir quoi défendre, car toutes les données ne peuvent bénéficier de la même sécurité. »