Sécurité des réseaux Wi-Fi : un défi multiforme

Les réseaux sans fil sont devenus ces dernières années une cible de choix pour les pirates, qui s'efforcent toujours de s'engouffrer dans les failles existant dans la chaine de sécurité des entreprises et des organisations. Concrètement, les réseaux Wi-Fi d'entreprise, au sens large, sont aujourd'hui confrontés à six catégories identifiées de menaces.

1 – Les points d'accès Evil Twin

Technique connue depuis de nombreuses années mais remise au goût du jour, un point d'accès Evil Twin prend la place en toute discrétion d'un point d'accès légitime en imitant son identifiant SSID et son adresse MAC. Les pirates peuvent alors intercepter le trafic et s'immiscer dans les échanges de données, par exemple pour voler des identifiants ou des données, ou encore infecter les ordinateurs des victimes.

2 – Les points d'accès mal configurés

Lors de l'installation de nouveaux points d'accès Wi-Fi, des erreurs involontaires de configuration sont toujours possibles, par exemple en laissant les paramètres par défaut, ou en maintenant un SSID privé ouvert et sans chiffrement, ouvrant la voie à des interceptions de données sensibles.

3 – Les points d'accès illicites

Il s'agit de points d'accès Wi-Fi qui ont été installés sur un réseau sécurisé sans autorisation explicite d'un administrateur. Ces points d'accès se connectent au réseau autorisé, en général au moyen d'un SSID ouvert, et permettent aux pirates de contourner le système de sécurité de l'entreprise.

4 – Postes clients illicites

Tout poste client connecté à un point d'accès illicite ou malveillant à portée d'un réseau sans fil privé, par exemple dans un café ou un restaurant, peut être considéré comme illicite. Il peut avoir fait l'objet d'attaques de type « Man in the middle » et avoir été infecté par des malwares et autres ransomwares. Une fois ce poste ou terminal client reconnecté à un point d'accès légitime, il pourra diffuser son ou ses malwares dans le réseau d'entreprise.

5 – Les points d'accès voisins

Un poste client autorisé qui se connecte à un point d'accès externe dans le voisinage peut contourner ainsi le périmètre de sécurité de l'entreprise et les restrictions de sécurité définies par le firewall. Par exemple, des employés qui décident pour une raison ou une autre de connecter leur smartphone au réseau du café d'en bas contournent en toute simplicité le périmètre de sécurité que leur entreprise a installé sur son réseau, ce qui peut permettre à des pirates de s'y infiltrer.

6 – Les réseaux ad hoc

Il s'agit de réseaux Wi-Fi « peer to peer » qui permettent à deux postes clients ou plus de communiquer directement entre eux, contournant ainsi les politiques de sécurité de l'entreprise et rendant le trafic totalement invisible. Ces réseaux ad hoc, simples à installer en quelques clics, peuvent avoir de graves conséquences juridiques pour les entreprises.

Pour contrer ces menaces, les entreprises ont plus que jamais besoin d'installer un environnement Wi-Fi de confiance, basé sur trois piliers :
– une performance de haut niveau, garantissant une parfaite expérience utilisateur
– une gestion évolutive, permettant de faire grandir le réseau en fonction des besoins
– une protection garantie de bout en bout contre toutes les catégories de menaces.