Cyberattaques IoT : Berlin et Londres plus exposées que Paris ?

Dans les grands pôles urbains des millions d'objets connectés « vulnérables » constituent une cible de choix pour les pirates informatiques, observe Trend Micro dans une étude. En Europe, deux villes parmi les plus dynamiques – Berlin et Londres – sont les plus exposées.

Pour aboutir à cette conclusion, l'éditeur japonais de solutions de sécurité s'est intéressé aux dispositifs visibles sur Internet. Et ce via une recherche réalisée sur le moteur spécialisé Shodan.io. Celui-ci indexe les objets et périphériques connectés (leur adresse IP et d'autres données sont donc visibles). Et effectue un scan automatique des ports.

Des ports ouverts et des dispositifs peu protégés augmentent l'exposition au risque d'attaques (par déni de service distribué ou DDoS, par ransomware, etc.).

En Europe de l'Ouest, Berlin (2,8 millions de systèmes visibles) et Londres (2,5 millions) sont les deux villes sur dix étudiées les plus exposées au risque de cyberattaques. Madrid (avec 1,3 million d'appareils), Amsterdam (plus de 948 500) et Athènes (543 400), suivent.

Derrière Oslo (432 800), Paris occupe la 7e position de ce classement européen des « actifs cyber exposés » avec 416 733 appareils « vulnérables » indexés. Lisbonne (plus de 409 000), Stockholm (405 800) et Rome (296 700) ferment la marche.

Imprimantes, webcams et PBX

Les imprimantes et les autocommutateurs téléphoniques privés (PBX) font partie du plus grand nombre de dispositifs vulnérables en Europe de l'Ouest. Avec les points d'accès sans fil, les pare-feux, les webcams et autres caméras IP. *« Il a suffi de quelques recherches sur Shodan pour identifier de nombreux flux de webcams [de particuliers et d'entreprises] visibles publiquement via un accès à distance non authentifié »,* explique Trend Micro dans son rapport.

Du côté logiciel, se sont les serveurs web HTTP (comme Apache HTTPD, Nginx, OpenSSH et Microsoft IIS) qui sont les plus exposés.

« *Des actifs cybernétiques exposés ne sont pas forcément compromis. Mais, le fait qu'ils soient exposés signifie que certains dispositifs, systèmes ou réseaux sont mal configurés. Visibles sur Internet, ces appareils sont vulnérables et peuvent donc être compromis* », prévient l'éditeur.

Ces résultats sont préoccupants pour les particuliers et les entreprises. Ces dernières sont notamment appelées à se mettre en conformité avec le Règlement général sur la protection des données (RGPD ou GDRP en anglais). Un texte qui entrera en vigueur le 25 mai 2018.

Lire également :

[IoT et sécurité: Sopra Steria et IOTA unis par la blockchain]

[Sécurité et IoT : pourquoi le pire est encore à venir]

crédit photo © adike / shutterstock