Les routeurs WiFi, de vraies passoires en matière de sécurité

Les routeurs constituent une porte d'entrée grande ouverte de la vie privée des utilisateurs. Tel est le message qu'a voulu faire passer l'éditeur de sécurité Avast qui tenait un point presse mercredi dernier que nos confrères d'*ITespresso.fr* ont suivi.

Selon l'entreprise installée en République tchèque, ces boîtiers qui concentrent les connexions entre les PC, smartphones, tablettes et autres objets connectés vers Internet, ouvrent l'accès des pirates aux différents appareils du réseau en cas de problème de sécurité physique, de faille logicielle ou de vulnérabilités dans les méthodes de chiffrement et d'authentification .

Le mot de passe, premier maillon faible

Le premier maillon faible dans cette chaîne semble être le mot de passe permettant d'accéder à l'interface d'administration du routeur : il est «trop faible dans 80 % des cas», rapporte Vincent «Vince» Steckler. Le CEO d'Avast (arrivé il y a six ans en provenance de Norton) ajoute que dans le monde, 63% des utilisateurs n'ont jamais modifié les informations de connexion par défaut de leur routeur.

Bilan : dans 45 % des cas, on retrouve l'identifiant «admin», associé à aucun mot de passe ou, à la rigueur, à la chaîne «password». De quoi faciliter la tâche des pirates. C'est sans compter le fait qu'une part non négligeable des quelques utilisateurs qui modifient le mot de passe en France choisissent leur nom, leur prénom ou leur date de naissance. Des informations faciles à dénicher par des techniques de social engineering.

Des routeurs vérolés ?

Autre point sensible : le firmware, c'est-à-dire le micrologiciel embarqué dans les routeurs… et dont les mises à jour sont souvent éludées par les constructeurs. Pratiquer le «reverse engineering» (analyse de code) peut permettre de détecter des failles de type zero-day, non corrigées et exploitables. Dans une étude publiée en février dernier, Tripwire (contrôle des configurations de sécurité système) estimait que 80 % des 25 modèles de routeurs sans fil les plus vendus sur Amazon à destination du grand public, des TPE et des indépendants présentaient un firmware vulnérable.

Qu'ils passent par l'une ou l'autre de ces deux voies, les pirates peuvent prendre intégralement le contrôle du routeur. Et le détourner pour renvoyer toutes les requêtes vers un serveur DNS malveillant, qui associera les URL saisies par l'utilisateur à des adresses IP malveillantes. Un processus particulièrement simple sur certains navigateurs comme Safari d'Apple, plus permissifs sur la vérification du chiffrement SSL («Secure Sockets Layer»).

Recommandations

Au gré de ses contributions blog, Avast distille d'autres recommandations concernant la sécurité du WiFi. Par exemple, contrôler régulièrement la liste des appareils connectés, activer le filtrage par adresses MAC et vérifier, surtout si le routeur est d'occasion, que le mode «Invité» n'est pas activé. Mais aussi masquer ou modifier le SSID (nom du routeur), qui peut trahir de nombreuses choses, dont la marque du produit, son emplacement ou les usages auxquels il est consacré. Autant de recommandations qui ne sont néanmoins pas à la portée de tous les foyers ou petites entreprises qui s'équipent en produits grand public.

Lire également

David Grout, McAfee : « sur la sécurité, les entreprises sont ambivalentes »
Les RSSI veulent faire du DSI un porte-parole de la sécurité
Sécurité : la DSI sous pression de la direction générale

crédit photo © Pavel Ignatov – shutterstock