



D'intelligente à hantée

Faits marquants et impressions du Forum Smart Home 2018 | Quel système choisir pour sa maison intelligente ? Comment la rendre sûre ? Quels sont les risques liés à l'intégration de plus en plus d'objets connectés ? L'événement organisé le 15 mars par Electrosuisse et l'IRB/GNI a fourni, entre autres, les réponses à ces questions.

TEXTE CYNTHIA HENGSBERGER

Selon Serge Le Men, ABB Solution SmartBuilding Newron, nous nous trouvons à l'aube de la troisième révolution ethnique. Après l'écriture et l'imprimerie, place à la révolution numérique et à l'établissement d'un monde ultraconnecté.

Ceci a un impact non négligeable sur le domaine de la construction. La planification et l'intégration d'un réseau de données devient, dès la conception du bâtiment, aussi essentielle que celles des réseaux électrique et hydraulique. En outre, les installations d'immatotique ou de domotique se trouvent de plus en plus liées à l'informatique et à l'Internet des objets. Or, qui dit connexion à Internet, dit

également risques liés au piratage informatique.

La version moderne de la maison hantée

Comme l'a démontré Daniel Berchtold, Hoo AG, l'intégration d'objets connectés aux systèmes domotiques peut exposer les réseaux informatiques privés à de sérieux risques si l'intégration n'est pas réalisée dans les règles de l'art.

Un exemple ? L'utilisation de Shodan, le « Google des pirates », un moteur de recherche spécialisé dans la détection d'objets connectés à Internet (serveurs, routeurs, mais aussi caméras ou autres périphériques). Lorsqu'un routeur avec des redirections de ports

est repéré, Shodan tente de pénétrer sur le réseau local afin d'analyser ce qui s'y trouve. Plus de 50 000 systèmes domotiques d'un fournisseur ont ainsi été touchés par Shodan il y a quelques années, et ce, simplement parce que les mots de passe par défaut n'avaient pas été changés. Un autre exemple ? En Suisse, 150 caméras privées d'un autre fournisseur sont actuellement facilement visibles sur Internet. Quand on sait qu'il suffit de cliquer sur un lien pour avoir accès à leurs images, cela fait froid dans le dos !

Sophos, un fournisseur de produits dédiés à la sécurité informatique, s'est pour sa part livré à une expérience édifiante : dans le cadre du projet Haunted

House (maison hantée), un domicile intelligent a été branché sans protection directement sur Internet et le trafic informatique y a été observé pendant un an. Résultat: jusqu'à 3800 tentatives d'accès quotidiennes et, à la fin du projet, la maison accueillait chaque jour plus d'un invité indésirable...

Des réflexes élémentaires

L'Internet des objets constitue une passerelle vers les réseaux. Il suffit d'un appareil mal protégé pour mettre en danger l'ensemble du réseau privé. Lors de l'intégration, il est donc essentiel de respecter quelques règles élémentaires: éviter autant que possible de connecter les systèmes à Internet, utiliser des réseaux (LAN ou VLAN) séparés pour les objets connectés et les autres périphériques, protéger chaque réseau avec un pare-feu, éviter les redirections de ports et utiliser une technologie VPN (virtual private network) pour les accès depuis Internet, attribuer une date d'expiration aux accès autorisés et effectuer régulièrement la maintenance, les sauvegardes et les mises à jour. L'établissement d'un contrat de service, à l'exemple de ceux rencontrés dans les domaines des chaudières, ascenseurs ou autres équipements, pourrait être une solution pour assurer avec professionnalisme la continuité de la sécurité informatique des installations domotiques.

Philippe Donnet, Défi Technique SA, l'a aussi souligné. Le réseau informatique doit être bien pensé, ordonné et protégé. N'y autoriser que les adresses MAC et IP des dispositifs qui doivent y avoir accès. Au niveau de la Suisse, Shodan voit plus de 2,7 millions d'objets connectés, dont probablement plus de 100 000 utilisent encore les noms d'utilisateur et mots de passe d'usine tels qu'admin/admin ou admin/1234. Le premier réflexe doit être de les changer! Il existe aussi des listes de recommandations pour la validation d'une installation (par exemple pour KNX). Autant les utiliser...

Le prochain Forum Smart Home en terre romande aura lieu en 2020. L'édition de 2019 se déroulera, quant à elle, à nouveau en Suisse alémanique.

Auteure

Cynthia Hengsberger est rédactrice Electrosuisse du Bulletin SEV/AES.
→ Electrosuisse, 8320 Fehraltorf
→ cynthia.hengsberger@electrosuisse.ch



Le Forum Smart Home a accueilli plus de 110 participants au SwissTech Convention Center.



Daniel Berchtold, Philippe Donnet et Pierre Kaufmann (de g. à d.) ont débattu des questions relatives à l'intégration de l'informatique dans la domotique.



Les produits présentés par les exposants ont ajouté une touche pratique.