

Augmenter la sécurité des maisons connectées

La cyber sécurité dans les maisons connectées est essentielle pour la sécurité des habitants et des visiteurs ponctuels. Cette étude de l'ENISA propose des bonnes pratiques visant à améliorer la sécurité des services et des appareils présents dans les maisons connectées.

À l'heure actuelle, les systèmes domotiques intelligents permettent de relier les appareils ménagers traditionnels à des dispositifs connectés qui collectent, échangent et analysent des données pour créer des services à valeur ajoutée et améliorer la qualité de vie des habitants.

De nouvelles cyber menaces pèsent sur les systèmes domotiques intelligents, telles que les programmes malveillants dans les téléviseurs connectés ou l'accès à distance aux babyphones, mettant ainsi en évidence notre dépendance à différentes technologies. Alors que les implications en termes de sécurité et de protection de la vie privée ne sont pas toujours évidentes pour les développeurs et les utilisateurs, elles peuvent pourtant avoir de vraies répercussions sur la vie, la santé et la sécurité des habitants et des visiteurs ponctuels.

Les maisons connectées font face à plusieurs défis : les fabricants historiques développent des objets connectés dotés de fonctionnalités innovantes mais n'investissent que peu pour garantir un fonctionnement sécurisé. Le développement rapide des appareils domotiques intelligents réutilise de nombreux composants tiers (matériel, logiciel et services), alors que l'on ne connaît encore mal les implications de l'utilisation de ces éléments clés.

Dans cette étude, l'ENISA propose une approche holistique présentant des bonnes pratiques concrètes pour sécuriser les services et les objets liés à la maison connectée. Ces mesures visent à protéger divers types d'appareils et de services connectés à un système domotique tout au long des différentes étapes de leur cycle de vie : depuis leur conception et leur intégration, à leur fin de vie, leur recyclage et leur destruction, en passant par leur phase d'utilisation et de maintenance. Parmi les bonnes pratiques, on retrouve notamment le test des fonctions de sécurité au stade de conception, l'appairage sécurisé des appareils au système domotique intelligent et l'assistance technique continue pour les mises à jour de sécurité.

Interrogé sur la cyber sécurité dans les maisons connectées, le Professeur **Udo Helmbrecht, Directeur Exécutif de l'ENISA, déclare : « Les maisons connectées évoluent à un rythme très rapide. Intégrer des appareils connectés dans un environnement existant implique de nouveaux défis en matière de sécurité, qui ont des conséquences sur la sécurité des habitants et des visiteurs de la maison connectée. Afin de garantir une sécurité maximale, les fabricants et les concepteurs doivent sécuriser le cycle de vie complet de leurs produits. »**



La maison connectée est une application centrale de l'« Internet des Objets » (IdO). À l'heure où la sécurité de l'IdO est de plus en plus importante, l'ENISA agit en développant des lignes directrices pour divers secteurs et champs d'application de l'IdO (*par ex.* transports en commun, voitures intelligentes etc.).

Pour lire le rapport complet (en anglais) : <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices>

Pour de plus amples informations techniques : Dr. Cédric Lévy-Bencheton, expert NIS, cedric.levy-bencheton@enisa.europa.eu

Pour toute demande de reportage presse et d'interview, veuillez contacter press@enisa.europa.eu, té. +30 2814 409576

