

Pensar en la seguridad del hogar inteligente es inteligente.

La ciberseguridad de los hogares inteligentes es esencial para garantizar la protección de los que los habitan o visitan. Este estudio de ENISA propone buenas prácticas en seguridad que mejoran la protección de dispositivos y servicios del hogar inteligente.

Los «entornos de hogar inteligente» complementan los electrodomésticos tradicionales con dispositivos conectados que recopilan, intercambian y procesan datos para crear servicios de valor añadido y mejorar la calidad de vida de sus habitantes.

Las nuevas ciberamenazas en los hogares inteligentes, como los programas malignos en las Smart TV o el acceso remoto a los intercomunicadores para bebés, ponen de manifiesto la dependencia de varias tecnologías. Como las implicaciones de seguridad y privacidad no siempre están claras para desarrolladores y usuarios, estas pueden acarrear consecuencias en la vida, salud y seguridad de sus habitantes y visitantes.

La domótica se enfrenta a varios desafíos: los fabricantes tradicionales desarrollan objetos conectados con funcionalidades innovadoras, pero se invierte muy poco en garantizar su seguridad. El rápido desarrollo de los dispositivos inteligentes para el hogar se basa en la reutilización de componentes de terceros (hardware, software y servicios). Sin embargo, las implicaciones de seguridad de estos elementos continúan siendo un aspecto complejo.

En este estudio, ENISA propone un enfoque integral con buenas prácticas aplicables para asegurar los dispositivos y servicios del hogar inteligente. Estas medidas pretenden proteger varios tipos de dispositivos y servicios presentes en los hogares inteligentes en las diferentes fases de su ciclo vital: el desarrollo, la integración y el uso, así como el mantenimiento hasta el final de su vida útil, su reciclaje o eliminación. Ejemplos de buenas prácticas incluyen la realización de pruebas de funciones de seguridad durante la fase de desarrollo, la comunicación segura entre dispositivos en el hogar inteligente, así como el apoyo continuo de actualizaciones de seguridad.

En relación a la ciberseguridad en los hogares inteligentes, Udo Helmbrecht, director ejecutivo de ENISA, comenta: «Los hogares inteligentes evolucionan rápidamente. Integrar dispositivos conectados a un entorno ya existente supone nuevos desafíos en seguridad con implicaciones en la protección de los habitantes y visitantes del hogar inteligente. Para garantizar la seguridad, los fabricantes y desarrolladores deben asegurar todo el ciclo de vida de sus productos».

La domótica es una aplicación importante del «Internet de las cosas» (IoT por sus siglas en inglés). Debido a la cada vez mayor importancia del IoT, ENISA responde desarrollando directrices para numerosos sectores y áreas de aplicación del IoT (p.ej. transporte público, coches inteligentes etc.).



Puede leer el informe completo aquí: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices>

Información técnica: Dr. Cédric Lévy-Bencheton, experto en seguridad de las redes y de la información (NIS), cedric.levy-bencheton@enisa.europa.eu

Para entrevistas y consultas relacionadas con la prensa, póngase en contacto con:
press@enisa.europa.eu, Tel.+30 2814 409576

