¿Es la ciberseguridad de los hogares inteligentes lo suficientemente inteligente?

El informe Panorama de amenazas y guía de buenas prácticas para hogares inteligentes y medios convergentes, publicado hoy por ENISA, supone una contribución importante a la consecución de los objetivos de la Estrategia de Ciberseguridad de la UE. Este estudio ofrece un planteamiento específico y bien enfocado, así como una visión general del estado actual de la ciberseguridad en el ámbito emergente de los hogares inteligentes. Su finalidad es identificar los retos y riesgos de seguridad, así como las contramedidas que requieren las tecnologías emergentes en los hogares inteligentes.

Para la elaboración de este informe se creó un grupo informal de expertos, que fue recopilando información en las diferentes etapas del proyecto. Asimismo, el estudio tiene en cuenta evaluaciones ya existentes y fuentes de información de dominio público, y ofrece un Panorama de amenazas temático en el ámbito de los hogares inteligentes.

Dentro del alcance del estudio, se han identificado agentes de amenaza que ponen de manifiesto varias fuentes de vulnerabilidad. Los ciberdelincuentes aparecen señalados como la principal categoría de amenaza, y también como la más hostil. El riesgo de violación de los hogares inteligentes debe considerarse como muy alto, dado el número cada vez mayor de dispositivos y hogares inteligentes y, en concreto, de medios convergentes. Asimismo, son varios los factores económicos que generan vulnerabilidades en la seguridad, en un momento en que existen diferentes diseños compitiendo en materia de costes y comodidad.

Muchos de los riesgos serán de tipo sociotécnico, debido a la profundidad y a la variedad de la información personal que puede captarse y procesarse, y generarán datos sobre actividades que previamente no se había registrado, con un estrecho vínculo entre las personas y sus entornos. Además, los intereses de los diferentes propietarios de activos en un hogar inteligente no tienen por qué ser necesariamente idénticos, sino que pueden incluso entrar en conflicto y crear un entorno complejo por lo que respecta a la actividad de la seguridad.

Por otro lado, la televisión y los medios convergentes generan problemas de seguridad con respecto a la conectividad, el funcionamiento integrado, los sistemas opacos y la incompatibilidad con los enfoques tradicionales en materia de seguridad de la información, además de otros problemas de privacidad, acceso y derechos de autor. Es probable que los dispositivos de medios convergentes sean unos de los primeros dispositivos de hogar inteligente que los consumidores introduzcan en sus hogares y, por lo tanto, se conviertan en el terreno donde se pongan de manifiesto muchos de los problemas identificados con relación a la seguridad de los hogares inteligentes.

No todos los hogares inteligentes se crean del mismo modo, principalmente debido a las diferentes rutas de diseño y a sus consiguientes particularidades con relación a la seguridad y la privacidad, así como a sus propios problemas y vulnerabilidades a la hora de compartir información. Tal y como sucede en muchos otros ámbitos de las TIC, la aplicación de unas medidas básicas puede aumentar significativamente la seguridad global en el ámbito del hogar inteligente.

Unas buenas prácticas en este sector implican diseñar el hogar inteligente como un sistema, prestar especial atención a la seguridad de los diseños de hogar inteligente basados en la nube, aplicar un marco de aislamiento (como los desarrollados para los vehículos inteligentes) y mantener los software críticos separados de las medidas de seguridad relativas a aplicaciones, redes y comunicaciones que no sean críticas. Enfoques como los utilizados con las redes inteligentes también podrían resultar aplicables en el contexto de los hogares inteligentes.

El Director Ejecutivo, Udo Helmbrecht, comentó: *"El hogar inteligente es un punto de contacto intenso entre la tecnología de la información en red y el espacio físico y, por lo tanto, aglutina los riesgos de seguridad procedentes de los contextos físico y virtual. Identificar las ciberamenazas es crucial para la protección del hogar inteligente y, en ese sentido, constituye un elemento clave para garantizar una implementación exitosa del hogar inteligente".*

Informe completo: Panorama de amenazas en hogares inteligentes y medios convergentes

Entrevistas y contacto con los autores: resilience@enisa.europa.eu, **consultas de medios de comunicación:** press@enisa.europa.eu

Notas para los editores:

Figura 1: Visión general de los activos de los hogares inteligentes y los medios convergentes, pág. 11.

Figura 2: Visión general de las amenazas asumidas por los activos de los hogares inteligentes, pág. 13.

Asociación entre las amenazas y los activos de los hogares inteligentes, pág. 34.

Tabla 1: Implicación de los agentes de amenaza en las amenazas, pág. 38.

Tabla 3: Medidas de buenas prácticas contra las categorías de amenazas, pág. 51.

Informe anual de ENISA sobre el Panorama de amenazas **2014**, **2013**, **2012**

Panoramas de amenazas temáticas de ENISA:

Panorama de amenazas y guía de buenas prácticas para la infraestructura de Internet (2014)

Panorama de amenazas y guía de buenas prácticas para redes inteligentes (2013)