Echt smart: So werden Smart Homes sicherer

Internetsicherheit ist für Smart Homes unabdingbar, damit diejenigen, die dort leben oder zu Besuch sind, nicht in Gefahr gebracht werden. Eine neue ENISA-Studie zum Thema empfiehlt bewährte Praktiken, die die Sicherheit von Smart-Home-Geräten und -Diensten verbessern.

„Smart-Home-Umgebungen" ergänzen derzeit traditionelle Haushaltsgeräte mit Einheiten, die Daten sammeln, austauschen und verarbeiten. So stellen sie Mehrwertdienstleistungen zur Verfügung und verbessern die Lebensqualität der Bewohner.

Aufkommende Bedrohungen aus dem Cyberspace, etwa Schadprogramme auf dem Smart TV, Fernzugriff auf Babyfone etc., zeigen allerdings, wie sehr Smart Homes von den verschiedenen Technologien abhängig sind. Wie wichtig Sicherheit und Privatsphäre sind, ist Entwicklern und Nutzern oftmals unklar, was Folgen für das Leben, die Gesundheit und die Unversehrtheit von Bewohnern und Besuchern haben kann.

Smart Homes stehen gleich mehreren Herausforderungen gegenüber. So entwickeln herkömmliche Hersteller verbundene Objekte mit innovativen Funktionsweisen, investieren aber nicht genug in die Gewährleistung ihrer Sicherheit. Die rasante Entwicklung von Smart-Home-Geräten verwendet Komponenten von Drittanbietern (Hardware, Software und Dienstleistungen) mehrfach, während die Sicherheitsauswirkungen dieser Module ein schwieriger Aspekt bleiben.

In ihrer Studie empfiehlt die ENISA einen ganzheitlichen Ansatz, der umsetzbare, gute Praktiken für die Sicherung von Smart-Home-Geräten und -Dienstleistungen umfasst. Diese Maßnahmen zielen auf den Schutz der vielfältigen Geräte und Dienstleistungen, die in Smart-Home-Umgebungen genutzt werden, ab, und zwar in jedem Abschnitt ihrer Lebenszyklen – von der Entwicklung über Integration, Nutzung und Wartung bis hin zum Gebrauchsende mit anschließendem Recycling oder Entsorgung. Beispiele für gute Praktiken sind das Testen von Sicherheitsfunktionen im Entwicklungsstadium, das sichere Peering von Geräten im Smart Home sowie der kontinuierliche Support in Form von Sicherheitsupdates.

Zum Thema Cybersicherheit für Smart Homes sagt Prof. Udo Helmbrecht, Geschäftsführender Direktor der ENISA: „Smart Homes entwickeln sich extrem schnell. Verbindende Geräte in eine bereits existierende Umgebung zu integrieren, bringt neue Sicherheitsherausforderungen mit sich, die Auswirkungen auf die Sicherheit von Bewohnern und Besuchern haben können. Deswegen müssen Hersteller und Entwickler das Thema Sicherheit während der gesamten Lebenszyklen ihrer Produkte berücksichtigen."

Smart Homes sind wichtige Anwendungen des „Internets der Dinge" (Englisch: Internet of Things, IoT). Da das Thema IoT-Sicherheit immer wichtiger wird, entwickelt die ENISA Richtlinien für ausgewählte IoT-Felder und -Anwendungsbereiche (etwa öffentlicher Personennahverkehr, Smart Cars, usw.).

Hier finden Sie den ganzen Bericht: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/smart-infrastructures/smart-homes/security-resilience-good-practices

Kontakt für technische Informationen: Dr. Cédric Lévy-Bencheton, NIS-Experte, cedric.levy-bencheton@enisa.europa.eu
Kontakt für Interviews und Presseanfragen: press@enisa.europa.eu, Tel.+30 2814 409576