09.02.2015
EPR06/2015
www.enisa.europa.eu

# Sind Smart Homes sicher?

ENISA hat eine Studie zur „Bedrohungslandschaft und Anleitung zum richtigen Umgang mit Smart Homes und integrierten Medien“ herausgegeben und leistet so einen Beitrag zum Ziel der EU Cyber Security Strategie.

Die Studie zielt darauf ab, Sicherheitsrisiken und Herausforderungen sowie benötigte Gegenmaßnahmen für Technologien in Smart Homes zu identifizieren. Sie bietet einen spezifischen und fokussierten Ansatz und einen Überblick über die aktuelle Sicherheitssituation in diesem Bereich.

Für die Erstellung des Berichts wurde eine formlose Expertengruppe gegründet, um in allen Projektphasen Beiträge sammeln zu können. Die Studie orientiert sich außerdem an bereits existierenden Untersuchungen und öffentlich zugänglichen Informationsquellen und bietet so eine Einsicht in die thematische Bedrohungslandschaft im Bereich der Smart Homes.

Im Rahmen der Studie konnten drei Ursachen festgestellt werden, die ein Grund für Sicherheitslücken sein können. Internetkriminelle werden demnach in die Kategorie mit dem größten Sicherheitsrisiko eingeordnet, während der mögliche Missbrauch von Smart Homes aufgrund der zunehmenden Zahl von Smart Geräten und konvergierten Medien ebenfalls als hoch eingestuft wird. Des Weiteren generieren wirtschaftliche Faktoren ebenfalls Sicherheitslücke, während bei Designfragen immer die Kosten und die Zweckmäßigkeit in Konkurrenz zueinander stehen.

Da es sich um persönliche Informationen handelt, die abgefangen und weitergegeben werden, haben die Risiken einen sozio-technischen Charakter. Dabei werden vormals nicht dokumentierte Daten generiert, die eine Verbindung zwischen den Personen und ihrer Umgebung herstellen. Die Interessen verschiedener Netzeigentümer in Smart Homes stimmen nicht immer überein sondern können in Konflikt stehen wodurch eine komplexe Gegebenheit für die Sicherheit entsteht.

Integrierte Medien und Fernsehen erhöhen das Sicherheitsrisiko in Bezug auf Verbindung, eingebaute Funktionen, undurchsichtige Systeme und Inkompabilität mit herkömmlichen Sicherheitsinformationen neben Problemen wie Privatsphäre, Zugang und Datenschutz. Geräte mit intergrierten Medien sind in der Regel die ersten Smart Home Geräte, die in vielen Haushalten eingeführt werden. Daher gelten sie als Hauptursache für viele der identifizierten Smart Home Sicherheitsprobleme.

Nicht alle Smart Homes sind gleich gestaltet, da es unterschiedliche Design Pfade mit speziellen Sicherheits- und Privatspähreeinstellungen und dementsprechend eigenen Schwachstellen gibt. Wie in allen Bereichen der ICT hilft auch hier die Anwendung von Basissicherheitsinformationen, um die gesamte Sicherheit im Smart Home zu verstärken.

Ein erfolgreicher Umgang in diesem Bereich beinhaltet die Konzeption des Smart Homes als System, die genaue Betrachtung der Sicherheit von cloud-basierten Smart Home Geräten, die Eingliederung in ein isoliertes Programmiergerüst (wie in Smart Autos) sowie kritische Software von

unproblematischen Apps, Netzwerken oder Sicherheitskommuniktaionsmitteln fernzuhalten. Ähnliche Ansätze beziehen sich auf intelligente Vernetzungen, die auch im Smart Home Bereich angewendet werden können.

Geschäftsführer Udo Helmbracht kommentiert: *"Das Smart Home ist ein Punkt intensiven Kontakts zwischen Netzwerkinformationstechnologie und materiellem Raum. Daher kommen hier Sicherheitsrisiken aus dem virtuellen und dem räumlichen Kontext zusammen. Es ist essentielle Cyber Bedrohungen zu identifizerien, um die Sicherheit des Smart Homes zu garantieren. Dies ist ein Schlüsselelement für den Erfolg des Smart Homes.*

Zur Studie: https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-for-smart-home-and-media-convergence/

Für Interviews und Anfragen an den Autor bitte resilience@enisa.europa.eu nutzen, für Presseanfragen press@enisa.europa.eu

Anmerkungen zu den Herausgebern:

Schaubild 1: Überblick der Smart Homes und konvergierter Medienverwertungen S. 11

Schabuild 2: Überblick der Gefahren von Smart Homes S. 13

Zusammenhang zwischen Gefahren und Medienverwertungen für Smart Homes S. 34

Tabelle 1: Einbindung der Gefahrenermittler in die Gefahren S. 38

Tabelle 3: Good-Practice-Maßnahmen gegenüber Gefahrenkategorien S. 51

ENISA Annual Bedrohungslandschaft 2014, 2013, 2012

Bedrohungslandschaft und Anleitung zum richtigen Umgang mit der Infrastruktur des Internets (2014)

Raster der Bedrohungslandschaft und Anleitung zum richtigen Umgang (2013)