idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Friedrich-Alexander-Universität Erlangen-Nürnberg
Dr. Susanne Langer

29.08.2017
http://idw-online.de/de/news680107

Forschungsergebnisse
Elektrotechnik, Informationstechnik
überregional

Wenn Fremde uns das Licht ausschalten

Smart Home-Produkte, wie beispielsweise Lampen, die über das Smartphone gesteuert werden, erfreuen sich in Privathaushalten einer stetig wachsenden Beliebtheit. Wenn allerdings Fremde plötzlich unsere Beleuchtung steuern, fühlen wir uns in unseren vier Wänden bedroht. Wissenschaftler des Lehrstuhls für IT-Sicherheitsinfrastrukturen der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) haben derartige Sicherheitsmängel in aktuellen smarten Lampen der Hersteller GE, IKEA, Philips und Osram aufgedeckt.

Dem Team um Philipp Morgner und Zinaida Benenson gelang es, Lampen verschiedener Hersteller für mehrere Stunden zum Blinken bringen – mit einem einzigen Funkbefehl aus einer Entfernung von über 100 Metern. Zudem beeinflussten sie die Lampen per Funkbefehl so, dass der Nutzer sie nicht mehr steuern konnte. Unter bestimmten Bedingungen war es sogar möglich, die Lampen aus der Ferne zu steuern und so beispielsweise die Lichtfarbe oder Helligkeit zu ändern.

Unzureichende Sicherheitsmaßnahmen
Die Schwachstelle haben die FAU-Sicherheitsforscher in einem wichtigen Funkstandard ZigBee für Smart Home-Produkte gefunden. Die Verbreitung von ZigBee-Produkten wird weltweit auf mehr als 100 Millionen Geräte geschätzt. Im Dezember 2016 wurden die aktuellsten Spezifikationen, ZigBee 3.0, der Öffentlichkeit vorgestellt. Ein Teil dieser Spezifikationen heißt Touchlink Commissioning und wird verwendet, um neue Geräte zu einem bestehenden Smart Home-Netzwerk hinzuzufügen, oder um ein neues Netzwerk einzurichten. Die Sicherheitsforscher haben gezeigt, dass Touchlink Commissioning unzureichende Sicherheitsmaßnahmen bietet und dadurch für Angriffe anfällig ist. In Zukunft werden wahrscheinlich auch sicherheitskritische Anwendungen wie Heizungsanlagen, Türschlösser und Alarmanlagen, die ebenfalls ZigBee nutzen, davon betroffen sein.

Hersteller reagieren auf Sicherheitsrisiko
Die Sicherheitsforscher empfehlen, Touchlink Commissioning in allen zukünftigen ZigBee 3.0 Produkten zu deaktivieren. Einige Hersteller haben bereits reagiert und stellen ihren Kunden ein Update zur Verfügung, das die Effekte der Angriffe deutlich verringert. Auf der folgenden Webseite werden aktuelle Informationen veröffentlicht:

www1.informatik.uni-erlangen.de/content/zigbee-security-research

Die Arbeitsgruppe der FAU beschäftigt sich mit der IT-Sicherheit für das Internet der Dinge. Die Beobachtung der Erlanger zeigt, dass Sicherheitsfragen für die Hersteller meist nachrangig zu Funktionalitäts- und Kompatibilitätsanforderungen sind. Deswegen analysieren die Erlanger vorhandene Schwachstellen und fordern die Hersteller dazu auf, bessere Sicherheitsmechanismen zu entwickeln.

Weitere Informationen:

Philipp Morgner

Tel.: 09131/85-69913
philipp.morgner@fau.de

Zinaida Benenson
Tel.: 09131/85-69908
zinaida.benenson@fau.de