So schnüffeln Sie zurück!

c’t-Raspion: Datenpetzen finden und bändigen

Hilfe zur Selbsthilfe ..... **Seite 16**
c’t-Raspion entdecken ..... **Seite 18**
Raspberry Pi herrichten ..... **Seite 22**
Offenherzige IP-Kamera ..... **Seite 24**
Morsende Steckdose ..... **Seite 26**
Plappernde Smart-TVs ..... **Seite 28**
Innenleben des c’t-Raspion ..... **Seite 30**

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

Alles ist ständig online und steht nicht grundlos unter Generalverdacht: IoT- und Smart-Home-Geräte werden in großen Massen zu kleinen Preisen in den Markt gedrückt. Wir zeigen, warum man solchen Geräten nicht blind vertrauen sollte und wie man ihnen auf den Zahn fühlen kann. Mit dem c’t-Raspion können Sie das auch.

Von Peter Siering

Regelmäßig landen smarte Geräte in den Testlaboren der c’t: Das Spektrum reicht von WLAN-Steckdosen vom Discounter zum Gegenwert einer Flasche trinkbaren Weins bis zu TV-Geräten der Preisklasse solider Gebrauchtwagen. Die meisten Geräte funktionieren ohne Zugang zum Internet nicht oder nur begrenzt. Oft sind Cloud-Dienste beteiligt, auch wenn das ohne aktive Anmeldung durch den Nutzer dort meist nicht offenkundig ist. Es lohnt sich deshalb genauer hinzuschauen.

Und je billiger Geräte sind, desto größer ist die Wahrscheinlichkeit, dass sie Sicherheitslücken enthalten. Die erlauben eine Übernahme durch Hacker, etwa um sie Teil eines Botnetzes werden zu lassen, oder können als Ausgangspunkt für Angriffe auf benachbarte Geräte dienen, etwa den Router. Experten halten es auch für möglich, dass gezielt manipulierte Geräte in Umlauf gebracht werden: Der Käufer schraubt dann eine WLAN-Lampe in die Fassung, ohne zu ahnen, dass die sofort Teil eines Botnetzes ist.

Bei sehr vielen Geräten ist das Risiko groß, dass beim Einrichten schon die ersten Daten in falsche Hände fallen: Damit etwa Smartphone-App und WLAN-Steckdose zueinander finden oder der Feinstaubsensor ins Netz kommt, müssen Sie sich über den Zugang zum heimischen WLAN verständigen. Oft ist das recht fahrlässig gelöst: Es werden offene WLANs verwendet, um die Daten zu übertragen, oder die Daten werden auf andere Art und Weise für andere mitlesbar übermittelt.

Häufig fließen auch Daten ab. Standardbibliotheken, die Entwickler einbinden, benutzen SDKs der großen Player: Google, Facebook, Microsoft, Apple & Co. – die übertragen gern mal allerlei statistische Daten, wie die Geräteart, Software-Versionen et cetera, aber auch GPS-Koordinaten, Werbe-IDs und so weiter. Der Nutzer einer Konfigurations-App für eine WLAN-Steckdose wird darüber eindeutig identifiziert und womöglich erkennt ihn der Hersteller als Kunden wieder, wenn der sich nach Staubsaugern umsieht.

Die Trackbarkeit spielt dann einer weiteren Eigenschaft in die Hand: unerwünscht eingeblendeter Werbung. Groß in diesem Geschäft ist Samsung. Die Smart-TVs des koreanischen Herstellers lassen keine Chance aus, den Käufer mit Werbung zu beglücken. Die Firma betreibt dafür eine eigene Vermarktungsplattform. So offensichtlich das beim Benutzen der Geräte ist, so schwierig ist es, diesen Teil der smarten Welt loszuwerden, ohne auf ihre Annehmlichkeiten zu verzichten.

Wie man sich wehren kann, haben wir in [1] gezeigt. Die folgenden Artikel widmen sich der Frage, wie man mehr über die Kommunikation der Geräte herausfinden kann. Wir stellen ein Werkzeug vor, mit dem die Redaktion Geräten auf den Netzwerkverkehr schaut. Es besteht aus einem Raspberry Pi und einem speziell zusammengeschnürten Softwarepaket. Wir haben das Projekt c’t-Raspion getauft.

Beim Beobachten des Netzwerkverkehrs braucht es Geduld und einen gewissen detektivischen Spürsinn, um außergewöhnliche Vorgänge zu erkennen und einzuordnen. Die folgenden Beispiele zeigen, worauf Sie achten müssen und wie Sie sich Gewissheit verschaffen. Wir ermuntern Sie als Leser, selbst zu forschen und Ihre Ergebnisse mit uns und anderen Lesern zu teilen, etwa in den Foren zu diesen Artikeln auf ct.de/y8mj. *(ps@ct.de)* c't

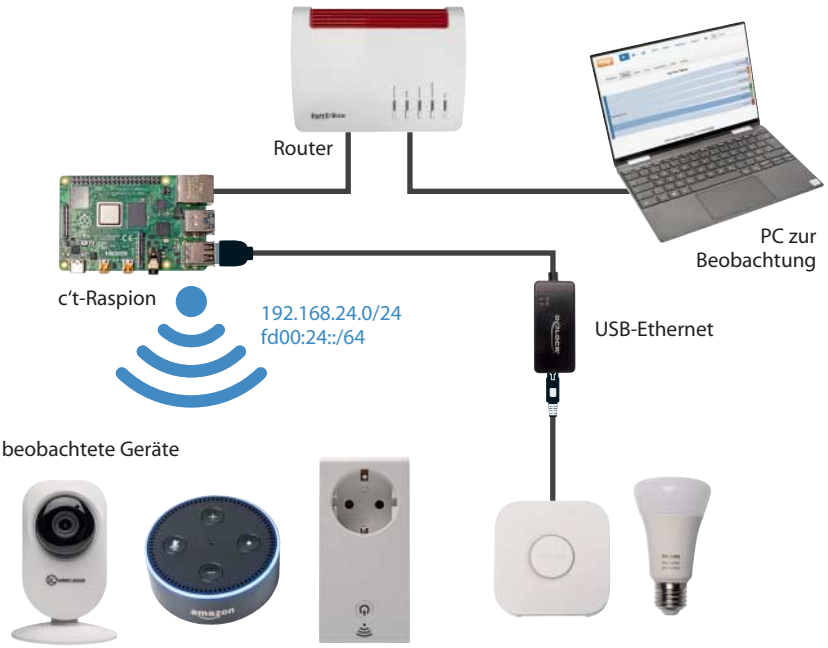
Literatur

[1] Peter Siering, Clever oder tumb?, Was Smart-TVs ins Internet übermitteln und wie leicht sie sich hacken lassen, c’t 25/2018, S. 74

***Foren:* ct.de/y8mj**

Netzwerkspion auf Basis eines Raspberry Pi

Unser Projekt c’t-Raspion spannt ein eigenes WLAN auf. Die Netzwerkaktivitäten dort eingebuchter Geräte können Sie im Webbrowser eines PCs verfolgen. Optional gelingt das auch für kabelgebundene Geräte, die der c’t-Raspion per USB-Ethernet-Adapter mit dem beobachteten Netz verbindet.



© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover