Ihre Smart-Home-Technologie überwacht Sie Tag und Nacht.

Jedes elektronische Gerät in Ihrem Zuhause – von Haushaltsgeräten über intelligente Zähler bis zu Türklingeln – bildet ein persönliches „Internet der Dinge“. Die großen Anbieter sammeln die Daten, tauschen sie aus oder verkaufen sie an andere – das ist das erwartete Ergebnis. Es bleibt jedoch eine Mischung aus Sicherheitsbedenken, die es Hackern ermöglicht, ein IoT-Profil von Ihnen zu erstellen, um zu sehen, wann Sie zu Hause sind, welche Wertsachen Sie haben könnten usw. Im Klartext: Sie sind nackt. Bildlich gesprochen sind Sie nackt wie ein Eichelhäher und jeder kann in Ihr Haus schauen.
Jedes größere Gerät in Ihrem Haus ist mit einer Wi-Fi-Karte ausgestattet (Kühlschränke, Klimaanlagen, Fernseher, Waschmaschinen, Trockner und intelligente Stromzähler). Ring- und Nestgeräte kommunizieren über Wi-Fi. Intelligente „Assistenten“ wie Ihr Smartphone, Alexa und Siri nutzen alle Wi-Fi. Da die meisten dieser Geräte nie mit Software oder Firmware aktualisiert werden, sind sie anfällig für Hacker.
Es überrascht nicht, dass KI als Lösung angesehen wird. Bereiten Sie sich darauf vor, mehr Geld zusätzlich zu Identitätsdiebstahl, Titelsperren, Virenschutz, Malware-Software usw. auszugeben. ***-*** *TN-Redakteur*

Internationale Forscher warnen eindringlich vor den Sicherheits- und Datenschutzproblemen, die in intelligenten Häusern lauern. Unter der Leitung von IMDEA Networks und der Northeastern University konnten die Wissenschaftler eine Vielzahl von Sicherheits- und Datenschutzbedrohungen aufzeigen, die sich aus den lokalen Netzwerkinteraktionen von Internet-of-Things-Geräten (IoT) und mobilen Anwendungen ergeben.

Smart Homes entwickeln sich ständig weiter und umfassen eine breite Palette von IoT-Geräten für Verbraucher, darunter Smartphones, Smart-TVs, virtuelle Assistenten und CCTV-Kameras. Diese Geräte sind mit Kameras, Mikrofonen und verschiedenen

Sensoren ausgestattet, die in der Lage sind, Aktivitäten in unserem intimsten Bereich – unserem Zuhause – zu erfassen. Aber können wir diesen Geräten wirklich vertrauen, dass sie die von ihnen gesammelten sensiblen Daten verarbeiten und schützen?

„Wenn wir darüber nachdenken, was hinter unseren Hauswänden passiert, denken wir an einen vertrauenswürdigen und privaten Ort. In Wirklichkeit durchdringen intelligente Geräte in unseren Häusern diesen Schleier des Vertrauens und der Privatsphäre auf eine Art und Weise, die es fast jedem Unternehmen ermöglicht, zu wissen, welche Geräte sich in Ihrem Haus befinden, wann Sie zu Hause sind und wo sich Ihr Haus befindet“, sagte David Choffnes, außerordentlicher Professor für Informatik und geschäftsführender Direktor des Cybersecurity and Privacy Institute an der Northeastern University, in einer Pressemitteilung. „Diese Verhaltensweisen sind den Verbrauchern in der Regel nicht bekannt, und es besteht ein Bedarf an besserem Schutz in den eigenen vier Wänden.“

Alarmierende Erkenntnisse über Smart Home“-Technologie

Für die Studie untersuchten die Forscher die Feinheiten der lokalen Netzwerkinteraktionen zwischen 93 IoT-Geräten und mobilen Anwendungen und konnten zahlreiche bisher unbekannte Sicherheits- und Datenschutzprobleme mit Auswirkungen auf die reale Welt aufdecken.

Entgegen der landläufigen Meinung, dass lokale Netzwerke sichere Umgebungen sind, zeigt die Studie neue Bedrohungen auf, die mit der unbeabsichtigten Offenlegung sensibler Daten durch IoT-Geräte in lokalen Netzwerken verbunden sind, die Standardprotokolle wie UPnP oder mDNS verwenden. Zu diesen Bedrohungen gehört die Offenlegung von eindeutigen Gerätenamen, UUIDs (Universally Unique Identifiers) und sogar des geografischen Standorts von Haushalten. Diese Informationen können von Unternehmen, die im Überwachungskapitalismus tätig sind, ohne das Wissen der Nutzer ausgenutzt werden.
„Bei der Analyse der von IoT Inspector gesammelten Daten haben wir Beweise dafür gefunden, dass IoT-Geräte unbeabsichtigt mindestens eine PII (Personally Identifiable Information) wie eine eindeutige Hardware-Adresse (MAC), UUID oder einen eindeutigen

Gerätenamen in Tausenden von Smart Homes in der realen Welt preisgeben“, erklärt Vijay Prakash, Mitautor der Studie und Doktorand an der Tandon School of Engineering der New York University. „Jede einzelne PII ist nützlich, um einen Haushalt zu identifizieren, aber die Kombination aller drei macht ein Haus sehr einzigartig und leicht identifizierbar. Zum Vergleich: Wenn man den Fingerabdruck einer Person mit der einfachsten Browser-Fingerabdrucktechnik nimmt, ist er so einzigartig wie einer von 1.500 Menschen. Wenn ein Smart Home mit allen drei Arten von Identifikatoren einen Fingerabdruck erhält, ist es so einzigartig wie eines von 1,12 Millionen Smart Homes“.

Die mächtige Waffe der lokalen Netzwerkprotokolle

Die Studie hebt hervor, wie lokale Netzwerkprotokolle als Seitenkanäle genutzt werden können, um auf Daten zuzugreifen, die theoretisch durch die Berechtigungen mobiler Anwendungen geschützt sind, wie den Standort von Haushalten.

„Ein Seitenkanal ist eine raffinierte Methode, um indirekt auf sensible Daten zuzugreifen. Entwickler von Android-Apps müssen etwa die Zustimmung der Nutzer einholen, wenn sie auf Daten wie den Standort zugreifen wollen“, erklärt Narseo Vallina-Rodriguez, Associate Research Professor bei IMDEA Networks und Mitbegründer von AppCensus. „Wir haben jedoch gezeigt, dass bestimmte Spyware-Anwendungen und Werbefirmen lokale Netzwerkprotokolle missbrauchen, um ohne Wissen des Nutzers auf diese sensiblen Informationen zuzugreifen. Alles, was sie machen müssen, ist, andere IoT-Geräte, die im lokalen Netzwerk über Standardprotokolle wie UPnP verwendet werden, freundlich zu fragen“.

„Unsere Studie zeigt, dass die von IoT-Geräten verwendeten lokalen Netzwerkprotokolle nicht ausreichend geschützt sind und sensible Informationen über das Zuhause und die Nutzung der Geräte preisgeben“, ergänzt Juan Tapiador, Professor an der Universidad Carlos III de Madrid. „Diese Informationen werden auf undurchsichtige Weise gesammelt und erleichtern die Erstellung von Profilen über unsere Gewohnheiten oder unseren sozioökonomischen Status“.

Breitenwirkung und Handlungsbedarf

Die Auswirkungen dieser Forschung gehen über den akademischen Bereich hinaus und unterstreichen die Notwendigkeit, dass Hersteller, Softwareentwickler, Betreiber von IoT- und Mobilfunkplattformen sowie politische Entscheidungsträger entschiedene Maßnahmen ergreifen, um den Datenschutz und die Sicherheit von Smart-Home-Geräten und Haushalten zu verbessern. Die Forscher haben diese Probleme bereits verantwortungsbewusst gegenüber den Herstellern gefährdeter IoT-Geräte und dem Android-Sicherheitsteam von Google offengelegt, was zu Sicherheitsverbesserungen bei einigen dieser Produkte geführt hat.

QUELLE: YOUR ‘SMART HOME’ TECHNOLOGY SPIES ON YOU DAY AND NIGHT