Neue Kooperation: Check Point und LG schützen Smart Home

Nach Entdeckung von kritischen Schwachstellen durch Check Point in LG SmartThinQ® Smart Home Lösung hat man gemeinsam Massnahmen ergriffen

SAN CARLOS, KA – 26. Oktober, 2017 – Check Point® Software Technologies Ltd. (NASDAQ: CHKP), der weltweit führende Anbieter von Cybersicherheitslösungen, präsentiert heute die Schwachstelle HomeHack in der Smart Home-Lösung LG SmartThinQ®. Dem Research Team von Check Point gelang es, die Kontrolle über die Appliance zu übernehmen und angeschlossene Geräte zu kontrollieren. Die LG SmartThinQ®-Appliance wurde millionenfach verkauft und viele Nutzer sind von HomeHack betroffen.

Der Angriff wurde durch Schwachpunkte in der LG SmartThinQ App für Mobilgeräte und in der Cloudapplikation ermöglicht. Das Team von Check Point hatte dabei Erfolg, sich in die SmartThinQ Cloud Applikation per Fernzugriff einzuloggen und von dort aus die Nutzeraccounts von LG-Kunden zu übernehmen. Mit diesen Zugängen konnten dann alle vernetzten Geräte im Haus des Opfers ferngesteuert werden.

Das Video zeigt, wie ein Saugroboter samt integrierter Videokamera übernommen wird. Durch die Zugriffsrechte über das Benutzerkonto können Geräte wie Kühlschränke, Öfen, Waschmaschinen, Trockner oder Klimaanlagen durch die Angreifer ferngesteuert werden.

Im Falle einer Übernahme des Home-Bot Saugroboters fällt eine Ausspionierung der Opfer sehr leicht, da der Staubsauger eine Videokamera mit Live-Stream-Funktion als Teil des HomeGuard-Angebots installiert hat. Die Webcam war eigentlich als Sicherheitsfeature für die Nutzer gedacht, wurde aber so Spionagetool der Angreifer.

“Je mehr smarte Geräte wir in unserem Zuhause einsetzen, desto stärker fokussieren sich die Angreifer auf die Verwaltungsprogramme anstatt auf die einzelnen Endpunkte. Durch Apps haben die Cyberkriminellen wesentlich mehr Möglichkeiten, Nutzer zu attackieren und persönliche Daten abzufangen. “, so Oded Vanunu, Head of Products Vulnerability Research bei Check Point. “Die User müssen sich dem Sicherheitsrisiko bewusst sein, welches mit der Nutzung von IoT-Geräten einhergeht. Besonders wichtig ist zudem, dass die Hersteller von IoT-Geräten richtige Schutzmechanismen während der Entwicklung der Geräte und der Software integrieren.”

Die Sicherheitsmängel in der SmartThinQ Mobile App nutzte Check Point, um einen gefälschten LG-Account zu erstellen und dann damit echte LG-Konten zu übernehmen. Check Point informierte LG am 31. Juli 2017 und die Schwachpunkte wurden bis Ende September 2017 durch LG beseitigt. “Glücklicherweise reagierte LG sehr verantwortungsbewusst und stellte eine umfangreiche Beseitigung der Schwachstelle für die Appliance und die App bereit.”, teilt Oded Vanunu mit.

„Wir sehen sichere Software als wichtige Aufgabe an und Teil unserer Mission: Die Verbesserung des Lebensstandards der Nutzer weltweit. Deshalb erweitern wir gleichzeitig unsere Line-Up und Smart Home-Lösungen und entwickeln zeitgleich zuverlässige Apps für unsere Produkte,“ sagt Koonseok Lee, Manager Smart Development Team, Smart Solution BD, LG Electronics. “Im August arbeiteten LG Electronics und Check Point Software Technologies zusammen an einer umfangreichen Sicherheitsanalyse, um mögliche Schwachpunkte zu finden und zu beseitigen. Das Ergebnis sind mehrere Updates und seit 29. September 2017 läuft die Version 1.9.20 ohne Probleme. LG Electronics wird seine Schutzmechanismen in der Software und die Kooperation mit Cybersicherheitsexperten wie Check Point weiter ausbauen, um die eigenen Produkte besser und sicherer zu machen.“

Um sich vor Angriffen zu schützen, sollte die LG SmartThinQ App und Appliances geupdated werden, die Software dazu steht auf der LG-Homepage zur Verfügung. Check Point empfiehlt Nutzern zudem folgende Schritte, um ihr Smart Home und Wi-Fi gegen Attacken zu schützen:

1. Bringen Sie ihre LG SmartThinQ App auf den neuesten Stand (Version 1.9.23). Das Update kann via Google Play Store, Apples App Store oder über die LG SmartThinQ App unter Einstellungen eingespielt werden.
2. Updaten Sie Ihre Smart Home Appliance mit der neuen Firmware. Klicken Sie dazu auf das Smart Home Produkt unter SmartThinQ Applikation Dashboard (Falls ein Update verfügbar ist sollte ein Popup-Fenster erscheinen).

LGs SmartThinQ® erfreut sich grosser Beliebtheit, da das eigene Zuhause mobil und jederzeit über das Smartphone überwacht werden kann. Alleine der Home-Bot Saugrobotor wurde im ersten Halbjahr 2016 über 400‘000 Mal verkauft. Im letzten Jahr wurden zudem 80 Millionen Smart Home Devices an den Mann gebracht, das entspricht einem Wachstum von 65 Prozent.

Check Points Ressourcen zur Gefahrenabwehr und Details zum Research finden Sie auf:
https://blog.checkpoint.com/

Folgen Sie Check Point auf:
Check Point Blog: http://blog.checkpoint.com/
Twitter: http://www.twitter.com/checkpointsw
Facebook: http://www.facebook.com/checkpointsoftware
YouTube: http://www.youtube.com/user/CPGlobal
LinkedIn: https://www.linkedin.com/company/check-point-software-technologies

Über Check Point Software Technologies
Check Point Software Technologies (www.checkpoint.com) ist der grösste Pure-Play Netzwerk- und Cybersicherheitsanbieter weltweit. Als Marktführer der Cybersicherheitsbranche bietet Check Point die führende Technologie und schützt seine Kunden vor Cyberattacken mit einer unschlagbaren Fangquote bei Malware und anderen Bedrohungen. Check Point bietet eine umfassende Sicherheitsarchitektur, um Unternehmen zu schützen. Egal, ob Netzwerk oder Mobilgerät – Check Point deckt alle Bereiche ab und kann diese über seine leicht verständliche Sicherheitsmanagementplattform verwalten. Über 100‘000 Organisationen vertrauen auf den Schutz von Check Point.
Check Point Alps (Schweiz und Österreich) mit Sitz in Zürich und Wien beschäftigt mehr als 30 Mitarbeitende.

Pressekontakt:
Check Point Software Technologies (Switzerland) AG
Sonja Meindl
Tel: +41 44 316 64 44
E-Mail: smeindl@checkpoint.com

Jenni Kommunikation
Sylvana Zimmermann
Tel: +41 44 388 60 80
E-Mail: sylvana.zimmermann@jeko.com

