Von nichts kommt nichts: Der eigene 4G Hotspot ist per se nicht sicher – aber man kann ihn sicherer machen.

Es ist eine Lebensweisheit, die man auch der IT-Sicherheit zugestehen darf: man muss sich kümmern, sonst läuft es aus dem Ruder. Eine kürzlich veröffentlichte Analyse zum Einsatz von 4G Hotspots zeigt deutliche Sicherheitslücken bei der Nutzung dieser Geräte. Wer sie verwendet, sollte sich ein paar Minuten Zeit nehmen, um Einstellungen und Verhalten einem Sicherheits-Check-up zu unterziehen.

Was ist ein 4G Hotspot?
Einfach gesagt ist ein 4G Hotspot eine Miniaturform des hauseigenen Routers, der batteriebetrieben und mit einer SIM-Karte ausgestattet ist. Ein klassischer Router verbindet sich typischerweise mit dem Telekommunikationsanbieter für die Internetverbindung und bietet Wi-Fi oder ein verkabeltes Netzwerk für Laptops, Desktop-Computer und sämtliche smarte Geräte. Im Gegensatz dazu sind 4G-Hotspots meist Geräte im Taschenformat, die nirgendwo andocken, außer um die internen Batterien aufzuladen.

Die Mehrheit der aktuellen Smartphones verfügen über eine Hotspot-Funktion. Damit lässt sich die 4G-Verbindung eines Handys via Wi-Fi nutzen, um beispielsweise andere Geräte ins Internet zu bringen. Dennoch sind eigenständige Hotspots nach wie vor beliebt, besonders weil sie es einfacher machen, Sprache und Datenkommunikation voneinander zu trennen. Viele Provider offerieren Angebote, bestehend aus Hotspot-System und Prepaid Daten-Sim-Karte, speziell für Nutzer, die zuhause kein Festnetz mehr möchten.

Wie steht es dabei um die Sicherheit?
Gibt es Firmware Upgrades oder Sicherheits-Patches? Wie sicher ist ein Hotspot-Gerät? Viele Leute tragen ein solches Helferlein gerne mit sich, um nicht auf die unzähligen und wenig vertrauenswürdigen öffentlichen Access Points in Einkaufszentren, Hotels und Cafés angewiesen zu sein.

Theoretisch ist diese Idee auch nicht die schlechteste. Denn es sollte tatsächlich sehr viel unwahrscheinlicher sein, über eine vom Nutzer selbst kontrollierte Wi-Fi-Verbindung, die direkt mit einem mobilen Netzwerk kommuniziert, gehackt zu werden, als über eines der öffentlichen Gratisangebote mit nicht bekannten Router-Einstellungen und Konfigurationen. In der Praxis hapert es aber auch bei den eigenen Hotspots oftmals am Fine-Tuning. Sie sind nur so sicher wie die getätigten Einstellungen und installierten Firmware-Upgrades. Nicht zu vernachlässigen ist dabei auch die Gefahrenquelle der Firmware-Version selbst, auf die der Nutzer zumeist keinen Einfluss hat, da sie fast immer vom Mobilfunk-Provider vorgegeben wird.

IoT-Geräte: Bei günstigen Modellen kann kaum in Sicherheit investiert worden sein
In den letzten Jahren wurden die Sicherheitslücken in Routern für das Heimnetzwerk und anderen Internet of Things (IoT)-Geräten vielfach analysiert und beschrieben. Es gibt eine Vielzahl an Gründen, warum IoT-Geräte nicht über den Standard an integrierter Sicherheit verfügen, den man sich dafür wünschen würde. Ein Grund mögen die Kampfpreise sein, mit denen Webcams und Co. angepriesen werden. Das IoT-Gadget für unter 20 Euro lässt nicht viel Spielraum für eine ernstzunehmende Sicherheitsfunktionalität. Einfacher Gebrauch sticht oft Funktion und Sicherheit aus. In einem umkämpften Consumer-Markt haben solche Geräte, die dem Nutzer nach dem Einschalten sofort Sicherheitsfragen stellen, oft weniger Chancen

als diejenigen, die gleich betriebsbereit sind. Nächstes Problem: Massenweise produzierte IoT-Geräte liegen oft eine ganze Weile im Lager oder Regal. Kommt es dann irgendwann aufs Kassenband, kann die Firmware bereits lange überholt und viele Sicherheitslücken ungepatched sein.

Sicherheitsfalle: Schadcode via Formular
So geschehen mit verschiedenen Hotspot-Geräten. Wie Pen Test Partners entdeckte, spielt das Thema Sicherheit bei mehreren Herstellen keine wirkliche Rolle, insbesondere im Web-Interface, das für Setup, Konfiguration und ironischerweise auch Updates genutzt wird. Im Gegensatz zum klassischen Router zuhause verfügen die transportablen Varianten nicht über einen eigenen Bildschirm oder eine Tastatur. Sie vertrauen sich einem kleinen Web-Server für ihr User-Interface an – und hier liegt das Problem: Viele dieser Web-Server nutzen potenziell leicht angreifbare Kommunikationswege, um Remote-Befehle entgegen zu nehmen. So kann oftmals via Web-Interface ohne großen Aufwand Schadcode über Formulare auf Betriebssysteme oder Datenbanken eingeschleust werden. Die Kommandos, ausgestattet mit Root-Rechten, können verheerenden Schaden anrichten. Extra-Accounts, unerwünschte Server-Prozesse, Löschen von Daten, Verändern der Firewall-Regeln, Passwort-Diebstahl – die Liste des möglichen Missbrauchs ist lang.

Was ist zu tun? Michael Veit, Security Experte bei Sophos, gibt Tipps, wie die Nutzung des eigenen 4G-Hotspots sicherer wird:

1. **4G-Hotspots so umsichtig behandeln wie das eigene Smartphone**
   Sie mögen günstiger und weniger leistungsfähiger sein, aber in der Sache sind 4G-Hotspots wie Smartphones. Der Nutzer sollte die gleiche Sorgfalt wie bei seinem Handy anwenden und verfügbare Softwareupdates sowie Patches umgehend einspielen.

2. **Augen auf nach Fehlerberichten**
   Als erstes sollten Nutzer herausfinden, welcher Hersteller das genutzte Hotspot-Modell entwickelt hat. Mobilfunkanbieter versehen die Geräte oft mit ihrem Logo, so dass Modellnummer und Hersteller nicht leicht zu finden sind. Hier helfen oft das Handbuch oder das Web-Interface weiter. Wenn Modell und Anbieter bekannt sind, kann online gezielt nach potentiellen Sicherheitslücken gesucht werden. Gegebenenfalls bietet sich auch die Einrichtung eines Alerts für mögliche Bugs an, um schnell informiert zu sein.

3. **Aktives Log-out**
   Dieser Rat gilt für sämtliche Online Services und entsprechend sollten sich auch 4G-Hotspot-Nutzer nach dem Bearbeiten der Router Einstellungen unbedingt aktiv auf dem Web-Interface abmelden. Denn auch diese Weblinks können in externe Webseiten eingebettet sein, die unter Umständen bösartig sind.

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos fast 400.000 Unternehmen jeder Größe in mehr als 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor kontinuierlich neu entwickelten Cybertaktiken und -techniken, einschließlich automatisierter Attacken, Ransomware, Malware, Exploits, Datenexfiltration, Phishing und mehr. Die preisgekrönte, Cloud-basierte Plattform Sophos Central integriert das gesamte Sophos-Produktportfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized Security System. Die Lösungen von Sophos sind exklusiv über den globalen Channel mit mehr als 47.000 Partnern und Managed Service Providern (MSPs) erhältlich. Sophos stellt seine Technologien für Unternehmen auch Privatanwendern mit Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de