soft S check

Un-Sicherheit von IoT-Devices

Am Beispiel von Reverse Engineering des TP-Link HS110

Die Angriffe von Internet of Things (IoT)-Geräten auf Router der deutschen Telekom und den DNS Betreiber Dyn haben erneut die völlige Unsicherheit dieser Geräte verdeutlicht. Sie wurden ausgelöst durch Malware wie Mirai, die Internet-basierte Webcams, Babyphones etc. kontrollierte.

In beiden Fällen waren die infizierten Geräten unzureichend zugriffsgeschützt und wurden schlussendlich als Angriffswerkzeuge ausgenutzt. Der Einsatz fest-programmierter (nicht auswechselbarer) Standard-Passwörter und in der Grundkonfiguration geöffneter Ports wird konsequenterweise von Kriminellen systematisch ausgenutzt.

Viele dieser Geräte sind auch weiterhin angreifbar: Mit dem TP-Link HS110 wurde ein IoT-Gerät zur Home Automation genauer betrachtet. Es handelt sich hierbei um eine Prozessor-gesteuerte Steckdose, die sich mit dem hauseigenen WLAN verbindet und per ebenfalls unsicherer Smartphone-App verwaltet wird. Zur Konfiguration stellt das Gerät einen ungesicherten Ad-Hoc Access Point zur Verfügung. Eine Kommunikation mit der Cloud des Herstellers ist ebenfalls vorgesehen und ermöglicht diesem, den Lebenszyklus (Gerätenummer, Eigentümer, Einsatzzeit und –dauer) eines jeden Geräts genau zu verfolgen. Der disassemblierte Firmware-Quellcode offenbart Details über die Implementierung, über die verwendeten Protokolle sowie im Klartext gespeicherte Standardpasswörter.

Mit Reverse-Engineering nach dem Black-Box-Prinzip wurde der Einsatz einer einfach-knackbaren XOR Verschlüsselung nachgewiesen. Daraus folgend kann die gesamte Kommunikation des Geräts leicht entschlüsselt werden. Zu diesen Informationen gehören auch die an die Cloud zur Registrierung gesendeten Zugangsdaten.

Durch die über die Kommunikation bekannten Informationen war es möglich, ein kleines Tool zur Steuerung des TP-Link HS110 zu entwickeln. Dieses kann ohne jegliche Authentifizierung beliebige Geräte der Serie steuern und beliebig manipulieren. Ein Wartungsprotokoll - mit entsprechendem offenem Port am IoT-Gerät - gibt weiterhin Auskunft über die Konfiguration und den Status des Geräts und kann spezielle gerätespezifische Befehle ausführen.

Der eingesetzte völlig unzulängliche Ansatz ‚Security by Obscurity‛ ist für eine umfassende Sicherheit des Geräts offensichtlich nicht ausreichend. Dies gewinnt weiter an Relevanz, da die Verwendung von Universal Plug and Play (UPnP) standardmäßig bei vielen Routern aktiviert ist. Die nicht ausreichend gesicherten Geräte aus dem Heimnetzwerk können so den Zugriff aus dem Internet ermöglichen.

Nachträgliche Korrekturen am Produkt führen unweigerlich zu zusätzlichem Aufwand und damit auch weit höheren Kosten. Eine frühzeitige Prüfung des Konzepts durch Threat Modeling, sowie intensive Prüfung durch Penetrationstests sind also auch aus Kostengründen unverzichtbar.

Eine technisch detaillierte Beschreibung findet sich unter
https://www.softscheck.com/en/reverse-engineering-tp-link-hs110/.