Wenn das Zuhause zum Büro wird:
Acht Schritte für die Sicherheit des Netzwerks daheim

Sophos hat acht wichtige Fragen zusammengestellt, mit deren Hilfe Nutzer ihr Netzwerk Schritt für Schritt sicher einrichten können.

Das mobile Arbeiten vom heimischen Schreib- oder Küchentisch aus bleibt uns sicher noch eine ganze Weile erhalten. Umso wichtiger ist es, gerade jetzt das Netzwerk, in dem sich Computer oder Laptop mit den jobrelevanten Daten befinden, gut zu schützen. Denn leider haben in dieser Zeit auch Cyberkriminelle Hochkonjunktur.

Jedes Mal, wenn ein nicht ausreichend geschütztes Gerät an ein Netzwerk angeschlossen wird besteht die Gefahr, dass Cyberkriminelle es aufspüren und es im schlimmsten Fall dazu nutzen, in das digitale Privat- oder Berufsleben eines Nutzers einzutauchen.
Der entscheidende Punkt, den viele Nutzer übersehen, ist dabei, dass hier nicht nur Laptop und Smartphone Einfallstore darstellen, sondern vor allem auch die ganzen anderen „Home Gadgets“.

IoT-Geräte beinhalten mehr Angriffsflächen als auf den ersten Blick sichtbar
Viele IoT-Geräte basieren auf dem Linux-Kernel und der Open-Source-Systemsoftware, die typischerweise den Kern jeder Linux-Distribution bildet. Tatsächlich enthalten aber selbst die kleinsten und simpelsten Geräte oft nicht nur Spezialsoftware, die auf dieses Gerät zugeschnitten ist, sondern auch eine Reihe von Standard-Unix-Befehlszeilen-Dienstprogrammen, die mit den Werkzeugen eines jeden Penetrationstesters identisch oder ihnen zumindest sehr ähnlich sind.

Beispielsweise enthält ein Gerät wie eine Webcam oder ein intelligenter Lautsprecher normalerweise nicht nur Audio- und Videoverarbeitungscode.
Was wahrscheinlich ebenfalls zu finden sein wird:

- Eine oder mehrere Befehlsshells. Shells wie Bash, Lash, Ash oder Dash erleichtern das Ausführen von Befehlsskripten zur Automatisierung von Systemverwaltungsaufgaben.
- LAN- und WLAN-Konfigurationsprogramme. Tools wie ifconfig, ip, iwlist und iwconfig erleichtern das Zuordnen und Konfigurieren von Netzwerkeinstellungen.
- Download-Werkzeuge. Programme wie curl und wget können nicht nur zum Herunterladen von Dateien über das Internet verwendet werden, sondern auch zum Hochladen gestohlener Daten auf externe Webseiten, normalerweise nur mit einem einzigen Befehl.
- Andere Skriptsoftware. Häufig anzutreffen sind Programmierwerkzeuge wie awk, mawk oder gawk, eine minimalistische Skriptsprache, mit der Internet-Clients und -Server geschrieben sowie Dateien in nur wenigen Codezeilen durchsucht werden können.
- Werkzeuge zur Zeitplanung. Mit Werkzeugen wie z.B. cron können Programme regelmäßig ausgeführt werden, auch wenn niemand angemeldet ist. Das Ziel ist z.B. Computer zu entdecken, die mit dem Netzwerk verbunden sind.
- Tools für Fernzugriff und Verschlüsselung. Viele IoT-Geräte enthalten sowohl SSH-Client- als auch -Server-Software wie ssh, sshd oder dropbear. Diese geben Gaunern die Möglichkeit, mit bereits vorhandener Software geheime, verschlüsselte

Netzwerktunnel in das betroffene Netzwerk hinein sowie aus diesem heraus zu erstellen.
- Netzwerk- und Kontopasswörter. Das Wi-Fi-Passwort wird möglicherweise in einer Klartextdatei auf dem Gerät gespeichert, z. B. /etc/wpa_supplicant.conf. Kennwort- oder Authentifizierungstoken für alle Konten, an die das Gerät angeschlossen ist, können ebenfalls zur Verfügung stehen.

Wie kann man das heimische Netzwerk selbst gut absichern?
Jetzt könnte man meinen, dass es für die Sicherung des eigenen Netzwerks des kombinierten Wissens eines IT-Managers, eines Experten für technischen Support, eines Penetrationstesters und eines Netzwerktechnikers bedarf. Das ist aber glücklicherweise nicht so.
Sophos hat acht Schritte und Fragen zusammengestellt, mit deren Hilfe Nutzer die Einrichtung und den Betrieb ihres Netzwerks für die Heimarbeit sicherer gestalten können.

1. Wird dieses Gerät tatsächlich online benötigt? Wenn nicht, aus dem Netzwerk entfernen, bzw. nicht in Dauerbetrieb halten und nur dann anschalten, wenn es benötigt wird.

2. Wie ist das Gerät zu aktualisieren? Dies sollte unbedingt bekannt sein. Auch ist es ratsam, nur Geräte von Herstellern zu verwenden, die Sicherheitsupdates gewährleisten. Tut ein Hersteller das nicht, ist es besser auf ein Modell eines anderen Anbieters zu wechseln.

3. Wie wird das Gerät konfiguriert? Es ist wichtig, sich zu informieren, welche Sicherheitseinstellungen verfügbar sind, wozu sie dienen und wie sie einzurichten sind (siehe Frage 2).

4. Sind riskante Standardeinstellungen geändert worden? Viele IoT-Geräte verfügen über aktivierte Remote-Fehlerbehebungsfunktionen, die Hacker missbrauchen könnten. Oft haben die Geräte vorinstallierte Standardkennwörter, die den Cyberkriminellen auf jeden Fall gut bekannt sind. Einige Router werden mit aktiviertem Universal Plug and Play ausgeliefert, wodurch versehentlich das Innere eines Netzwerks freigelegt werden kann. Vor Inbetriebnahme eines Geräts sollten daher erst die Standardeinstellungen geprüft und geändert werden (siehe Fragen 2 und 3).

5. Wie viele Daten sollen tatsächlich geteilt werden? Wenn das Gerät an einen Onlinedienst angeschlossen ist, ist es hilfreich zu wissen, wie viele Daten das Gerät teilt und wie oft. Vermutlich ist es für eine reibungslose Zusammenarbeit z.B. Mit Kolleg*innen gar nicht notwendig, alle Daten jederzeit zu hochzuladen. Deshalb sollte festgelegt werden, was tatsächlich geteilt wird (siehe Fragen 3 und 4).

6. Besteht die Möglichkeit, mit zwei Netzwerken zu arbeiten? Einige Heimrouter erlauben es, ein WLAN in zwei Netzwerke aufzuteilen, die separat verwaltet werden können. Eine gute Lösung ist hierbei, etwa die IoT-Heimgeräte in einem Gastnetzwerk und Arbeitscomputer wie Laptops in einem anderen Netzwerk zu platzieren (siehe Fragen 1, 2, 3, 4 und 5).

7. Kann die "Client Isolation" aktiviert werden? Einige Heimrouter verfügen über eine als "Client-Isolation" bezeichnete Option, die Geräte im Netzwerk gegeneinander abschirmt. Dadurch wird das Risiko verringert, dass eine Sicherheitslücke in einem Gerät dazu benutzt wird, andere Computer "von innen" anzugreifen (siehe Fragen 1, 2, 3, 4, 5 und 6).

8. Weiß ich, an wen ich mich bei einem Problem wenden kann? Wenn der Arbeitgeber eine IT-Abteilung hat oder technischen Support bietet, ist es wichtig, sich zu informieren, wer dort der Ansprechpartner ist und welche Informationen dieser am ehesten benötigt, um schnell reagieren zu können.

IT-Abteilungen, die sich um Mitarbeiter an entfernten Standorten kümmern, sollten es ihren weniger technischen Kollegen auf einfachem Wege ermöglichen, Ratschläge zur Cybersicherheit einzuholen oder verdächtige Aktivitäten zu melden. Hierfür reicht eine interne E-Mail-Adresse oder Telefonnummer, über die Benutzer einfach und effizient mögliche Angriffe melden können. So kann ein ganzes Unternehmen zu den Augen und Ohren des Sicherheitsteams werden.

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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