7 Tipps für Verbraucher:
Mehr Sicherheit im Internet der Dinge

Das Internet der Dinge mit seinen zahlreichen Geräten kann schön, praktisch und sinnvoll sein. Damit es auch noch sicher wird, hat Sophos 7 Tipps zusammengestellt.

Wiesbaden, 17.3. 2016 Geräte aus dem IOT-Umfeld sind in fast jedem Haushalt anzutreffen und es werden täglich mehr. Smart-TVs, -Home-Devices und alle Arten von Wearables halten Einzug in unser Leben und sollen es einfacher, wärmer, heller oder unterhaltsamer machen. Kaum anzutreffen ist allerdings das Bewusstsein um die Gefahren, die mit der Internetverbindung einhergehen.

Denn: ein guter Schutz ist gar nicht so einfach. Immerhin kann man nicht einfach eine kostenlose Antivirensoftware aus dem Internet auf eine Kamera oder einen Fernseher aufspielen und aktivieren. Was also tun?

Sophos empfiehlt 7 einfache Maßnahmen, mit denen die Nutzung von IOT-Geräten sicherer wird.

1. **Richten Sie Ihrem Internet der Dinge ein eigenes Netzwerk ein**
   Die Mehrzahl der „smarten“ Geräte nutzt WLAN, sie benötigen kein Kabel, um mit Smartphone oder PC zu kommunizieren. Hier findet die Kommunikation statt, daher sollte hier auch der Schutz ansetzen. Erlaubt der heimische Router das Einrichten eines Gastnetzwerks, sollten die IOT-Geräte unbedingt mit diesem verbunden werden. So bleiben die wichtigen Daten auf dem Computer und Tablet von fremdem Zugriff geschützt. Oder richten Sie einfach gleich einen Gastzugang für ihre smarten Geräte ein.

2. **Vermeiden Sie unkontrolliertes Plug & Play**
   Wer glaubt, Fremde können nicht wissen, ob und welche IOT-fähige Geräte im Haushalt sind, der irrt gewaltig. Über spezielle Suchmaschinen können Kriminelle private Kameras, Fernseher oder andere Smart Appliances leicht finden. Viele Geräte, z.B. Videokameras, versuchen eine Verbindung mit Firewall und Router herzustellen um sich einfacher mit dem Internet zu verbinden; und auf genau diese Weise sind sie leicht von außen zu finden. Um das zu verhindern, sollte die UPnP-Funktion (Universal Plug and Play) am Router ausgeschaltet werden.

3. **Aktualisieren Sie die Firmware**
   Eine regelmäßige Aktualisierung der Firmware ist für IOT-Geräte ebenso wichtig, wie für jeden anderen PC. Den Zeitaufwand hierfür sollte man unbedingt in Kauf nehmen, Informationen hierzu finden sich auf den Webseiten der Hersteller. Verbraucher sollten dies genau so regelmäßig durchführen, wie einen Batteriewechsel oder die Überprüfung der Rauchmelder.

4. **Wählen Sie Ihre Passwörter mit Bedacht**
Womöglich können Sie es nicht mehr hören, aber nachlässig ausgewählte Passwörter stellen ein enormes Risiko dar. Wählen Sie Ihre Passwörter sorgfältig aus und notieren Sie diese an einem sicheren Ort. Komplexität ist wichtig, Einzigartigkeit ebenso. Viele Geräte veröffentlichen Passwörter unabsichtlich, manchmal sogar auch das WLAN-Passwort. Nutzen Sie nie ein und dasselbe Passwort für mehrere Geräte.

5. **Muss das Gerät wirklich in die Cloud?**
Devices, die mit einem Cloud-Service arbeiten, sind häufig unsicherer, als solche Geräte, die man komplett von zuhause selbst steuern kann. Lesen Sie die Bedienungsanleitung sorgfältig, um herauszufinden, ob der Internetzugang wirklich nötig und sinnvoll ist, oder ob es andere Möglichkeiten gibt.

6. **Fernsehen auf allen Geräten?**
Möchten Sie einen neuen Smart-Fernseher kaufen, und haben aber schon eine Spielekonsole? Verbinden Sie Geräte nur mit dem Netzwerk, wenn es wirklich nötig ist. Nur weil Geräte theoretisch alles können, müssen sie nicht alles dürfen. Wählen Sie aus, von welchem Gerät aus Sie Filme streamen möchten und vermeiden Sie unnötige Internetverbindungen.

7. **Hände weg vom Firmennetzwerk**
Die Fotos von der letzten Firmenfeier sollen schnell ins Intranet? Nehmen Sie Ihr IOT-Gerät niemals mit in die Firma und verbinden es ohne Rücksprache mit der IT mit dem Firmennetzwerk. Viele Geräte beinhalten große Sicherheitsrisiken, die im allerschlimmsten Fall sogar personelle Konsequenzen haben können.

Autor: Chester Wisniewski, Senior Security Advisor, Sophos

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
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de