**Internet of Things: Security ist immer noch ein großes Fragezeichen**



Nun erklimmt die Digitalisierung die nächste Stufe: Einem Unternehmen geht es heutzutage nicht mehr darum, dass die Produkte oder auch Fabrikanlagen digital vernetzt sind - in erster Linie will man nun auf dem „Internet of Things“ basierende Geschäftsmodelle wie [auch Ökosysteme aufbauen](https://www.computerworld.ch/business/iot/industrial-iot-stand-dinge-1713800.html). In den Augen der Unternehmer ist das „Internet of Things“ - also das Internet der Dinge - zudem ein Erfolgsmodell, damit man in der heutigen Zeit überhaupt wettbewerbsfähig bleiben kann.

**Angriffsfläche wird von Tag zu Tag größer**

Weltweit haben Unternehmen sogenannte IoT-Geräte im Einsatz, damit sie die Effizienz steigern können. Schlussendlich kann eine zwischen den Geräten stattfindende Kommunikation auch eine nicht zu unterschätzende Hilfe sein, wenn es etwa darum geht, Arbeitsprozesse zu vereinfachen wie auch zu beschleunigen. Bis zum Jahr 2020 werden, so die aktuellen Prognosen, weltweit um die 20,4 Milliarden IoT-Geräte verwendet werden; innerhalb der nächsten 12 bis 16 Monate sollen es zudem 65 Prozent aller Unternehmen sein, die mit dem Internet der Dinge zu tun haben. Jedoch darf nicht außer Acht gelassen werden, dass mit dem Siegeszug der internetfähigen Geräte auch die Angriffsfläche größer wird. Die Implementierung des Internets der Dinge erfolgt nämlich schneller als die Entwicklung diverser Mechanismen, sodass die Geräte mitunter nicht zu 100 Prozent geschützt werden können.

Auch die Researcher von ThreatLabZ haben sich mit dem Thema befasst und sich zwischen März und April 2019 besonders intensiv mit dem Traffic beschäftigt, der ausschließlich von IoT-Geräten ausgegangen ist. Dabei hat man den Gerätetyp, die verwendeten Protokolle, die Standorte der Server und auch die Häufigkeit der ab- wie auch eingehenden Kommunikation und die IoT-Traffic-Muster untersucht. Des Weiteren befasste man sich auch mit dem Thema Sicherheit.

**Sicherheitslücken dürfen nicht unterschätzt werden**

Innerhalb von 30 Tagen wurden in weiterer Folge 56 Millionen Transaktionen verarbeitet - diese stammten von 270 unterschiedlichen IoT-Geräten [mit eigenen Wallets](https://kryptoszene.de/iota-wallet-vergleich/), wobei es 153 verschiedene Hersteller gab. Am Ende ergab die Analyse, dass über 1.000 Unternehmen mindestens ein IoT-Gerät besitzen, das Daten aus dem Netz des Unternehmens in das Internet überträgt. So gehörten IP-Kameras, Drucker, Smart-Uhren, Set-Top-Boxen, Smart TVs, IP-Telefone wie auch Datenerfassungsterminals und medizinische Geräte zu den am häufigsten erkannten Gerätekategorien.

52 Prozent aller kommunizierenden IoT-Geräte konnten in die Kategorie der „Digital Media Devices“ - dazu gehören etwa Videorecorder oder auch Set-Top-Boxen - eingeordnet werden. Mit 17 Prozent landeten die Smart TVs auf dem zweiten Platz; auf den dritten Platz landeten Smart Watches, die jedoch im Privatbesitz der User sind (8 Prozent).

Die wohl wichtigste Erkenntnis der Untersuchung? 90 Prozent haben die IoT-Transaktionen unverschlüsselt über sogenannte Klartext-Kanäle laufen lassen - man hat also nicht auf die sichere SSL-Verschlüsselung zurückgegriffen. Jedoch ist die Verwendung einer unverschlüsselten Kommunikation nur eine von vielen Schwachstellen: Sicherheitsexperten haben mitunter die schwachen oder bereits voreingestellten Passwörter als nicht zu unterschätzende Gefahrenquelle gesehen und auch darauf hingewiesen, dass zum Teil schon veraltete Bibliotheken genutzt werden.

**Wie kann man das Risiko reduzieren?**

Aufgrund der Tatsache, dass IoT-Geräte so natürlich ein ausgesprochen [leichtes Ziel für die Cyberkriminellen](https://www.psw-group.de/blog/hackerangriffe-2018/6673) sind, ist es wichtig, dass Unternehmen daran arbeiten, das Risiko zu reduzieren.

Man sollte unbedingt voreingestellte Passwörter löschen und durch sichere Passwörter ersetzen. Zudem ist es ratsam, wenn die Firmware immer auf den neuesten Stand gebracht wird. Des Weiteren sollten isolierte Netzwerke für IoT-Geräte zum Einsatz kommen, um so eine laterale Ausbreitung von Malware unterbinden zu können. Mitunter ist es auch empfehlenswert, wenn man auch regelmäßig den Netzwerk-Traffic absichert.

**Der Mensch stellt das größte Sicherheitsrisiko dar**



Das Internet der Dinge mag zwar für viele Unternehmen, und das ist auch völlig nachvollziehbar, eine große Erleichterung sein, weil so tatsächlich unzählige Arbeitsprozesse schneller wie auch einfacher werden, jedoch darf man das Sicherheitsrisiko nicht außer Acht lassen. Aufgrund der Tatsache, dass hier (fast) immer der Mensch das größte Sicherheitsrisiko ist, muss natürlich auch darauf geachtet werden, dass man seine Mitarbeiter schult. Das bedeutet also, man muss hier sehr wohl auch ganz klar kommunizieren, dass es am Ende der Mitarbeiter selbst ist, der entscheidet, inwieweit das Unternehmen von Hackern angegriffen werden kann.

Bilder:

https://pixabay.com/de/illustrations/hacker-hacken-internet-sicherheit-1944688/

https://pixabay.com/de/photos/ipad-tablette-technologie-kontakt-820272/