CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Das Problem IoT

Definition IoT

Das Internet of Things (IoT) ist die Bezeichnung für das Netzwerk physischer Objekte („Things“), die mit Sensoren, Software und anderer Technologie ausgestattet sind, um diese mit anderen Geräten und Systemen über das Internet zu vernetzen, sodass zwischen den Objekten Daten ausgetauscht werden können. Diese Geräte reichen von normalen Haushaltsgegenständen bis hin zu anspruchsvollen Industriewerkzeugen.

Definition IoT

Smarte Haushaltsgeräte

- Kühlschränke, Beleuchtung, etc.

Wearables

- Fitness Tracker, etc.

Industrielle IoT-Geräte

- Produktionsmaschinen

Smarte Verkehrssysteme

- Automobilsysteme (siehe Tesla)

Definition IoT

Gesundheits- und Medizinische Geräte

- Blutdruckmessgeräte, Implantate

Smarte Sicherheitssysteme

- Türschlösser mit Fingerabdruck Scanner, etc.

Smarte Städte und Gebäude

- Smarthomes, Straßenverkehrssysteme, etc.

Warum stellt IoT eine solch große Angriffsfläche dar?

Die Integrierung von Sicherheits- sowie Patch- und Updatemechanismen erhöht die Produktionskosten, doch senkt das Comfort-Level, wodurch der Verkaufspreis steigt und die Nachfrage sinkt. Dies führt dazu, dass der Aspekt der Sicherheit oft von Herstellern vernachlässigt wird.

Produktionskosten oder **Sicherheitsmechanismen**

Warum stellt IoT eine solch große Angriffsfläche dar?

- Zu leistungsschwache Hardwarekomponenten für starke Sicherheitmechanismen
- Schwache Authentifizierung (z. B. Standardnutzernamen- und Passwörter)
- Mangelnde Updates
- Geringe Privatsphäre durch Datensammlung
- Meist Nutzung schwacher Netzwerkprotokolle
- Oft physisch zugänglich für Angreifer

IT-Sicherheitsgegenmaßnahmen

Netzwerksegmentierung

- Abgesehen von Standardmethoden wie dem Ändern des Default-Passworts sollten IoT-Geräte stets in einem separaten Netzwerk platziert werden, abseits derjenigen, in dene sensible Daten und andere Assets gehandhabt werden.

Firewalls

- Anhand von Firewalls lässt sich der Datenverkehr und Zugriff auf IoT-Geräte regeln und auf das Notwendigste begrenzen.

IT-Sicherheitsgegenmaßnahmen

Physische Sicherheitsmaßnahmen

- Der Zugang zu Produktionsmaschinen, Smart-Geräten und dergleichen in Unternehmen sollte stets angemessen physisch gesichert sein, um direkte ungewollte Eingriffe zu verhindern.

IT-Sicherheitsgegenmaßnahmen

- Fitness tracking app Strava gives away location of secret US army bases
- Angriff auf Router & Co. - Marai-Botnetz übernimm Smart Devices
- Hacker steuern Jeep Cherokee fern
- Paar erlebt Hackerangriff auf Smart-Home-Geräte - plötzlich sprach ein Mann durch die Google Nest-Kamera zu ihnen

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm