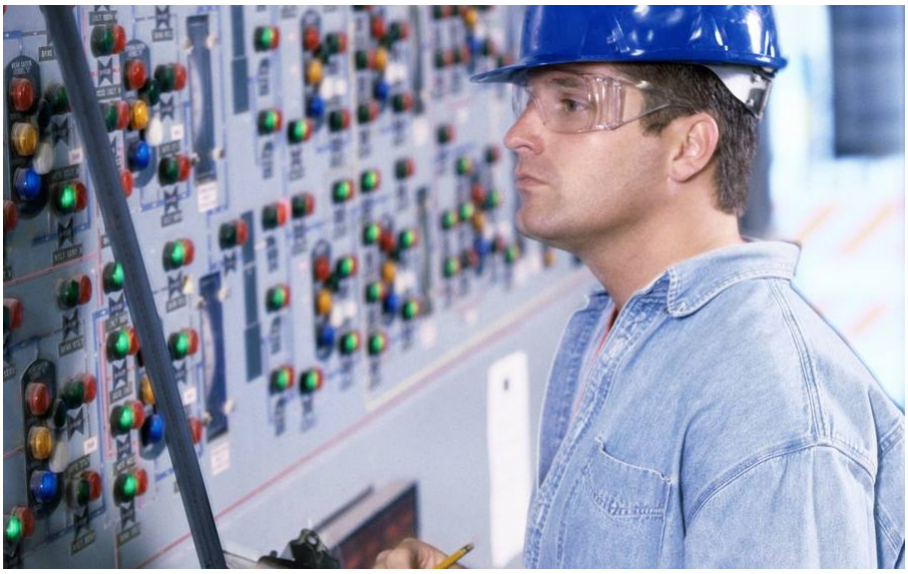
25.04.2016

IT DIRECTOR KRASSE IOT-SICHERHEITSLÜCKEN

Wie sicher ist das Internet der Dinge?

Von: Ina Schlücker

Wenn sämtliche Industrien und Geräte des täglichen sowie öffentlichen Lebens künftig über das Internet der Dinge (Internet of Things, IoT) miteinander vernetzt sein werden, lachen sich Cyber-Kriminelle ins Fäustchen. Gibt es für sie damit doch auf einen Schlag Milliarden neuer möglicher Angriffspunkte.



Wie sicher ist das Internet der Dinge?

Aktuell befindet sich das Internet der Dinge in einer Hype-Phase, in der viele Parteien ein großes Stück vom Kuchen abhaben wollen. Mittelständische wie Großunternehmen versprechen sich großen Profit oder befürchten, den Anschluss zu verlieren, sollten sie sich nicht mit IoT-Lösungen hervortun. „Dabei kümmern sich aktuell jedoch nur die Wenigsten um Sicherheit. Oft existieren heterogene Landschaften, in denen das schwächste Glied die Sicherheit des Gesamtsystems bestimmt. Und nicht zu vergessen gibt es die beiden Klassiker auch im IoT-Bereich: den Implementierungsfehler und die Hintertür", betont Rüdiger Kügler, Sicherheitsexperte der Wibu-Systems AG. Eine Problematik, die Darren Anstee, Chief Security Technologist bei Arbor Networks, nur allzu gut kennt. Seiner Ansicht nach werden auf einerseits viele Geräte entwickelt, ohne die notwendige Infrastruktur oder Funktionen bereitzustellen, um neu entdeckte Schwachstellen per Update zu beseitigen. Andererseits werden viele Geräte vernetzt und geraten dann einfach in Vergessenheit. „Es wird nur wenig Aufmerksamkeit auf ihre laufende Wartung und den Support verwendet", berichtet Darren Anstee.

IoT-Anlagen für Botnetze prädestiniert

Wie einfach es ist, IoT-Schwachstellen selbst ohne tiefere IT-Kenntnisse auszunutzen, zeigen laut Markus Merder Web-Seiten wie Shodan. Dahinter verbirgt sich eine IoT-Suchmaschine, mit der sich u.a. ungesicherte Webcams aufspüren lassen.

Hat man eine Schwachstelle ausgemacht, hängt die von den Hackern prädestinierte Methode von ihrer jeweiligen Zielsetzung ab. „Ist das Ziel das ‚Lahmlegen' eines Teilnehmers, einer Anlage oder eines Unternehmens, dann ist die Distributed-Denial-of-Service-Attacke (DDoS) die Waffe der Wahl", betont Rüdiger Kügler. Dabei wird ein Teilnehmer mit so vielen Anfragen quasi bombardiert, dass er nicht mehr antworten kann. Auch Darren Anstee sieht großes Potential für solche Attacken. „Denn DDoS-Angreifer suchen immer nach neuen Möglichkeiten, um die Größe und Komplexität ihrer Angriffe zu erhöhen. Mit Millionen von vernetzten Geräten entstehen Angriffsziele für neue und größere Botnets. Diese Gefahr wird mit der Zahl der Nutzer und ungepatchter Geräte noch weiter wachsen", so Anstee.

Ist das Ziel das Ausspähen von Daten oder deren Manipulation, dann sind die gewählten Methoden diffiziler und hängen von den gewählten Maßnahmen ab, so Kügler. Um entsprechende Informationen abgreifen zu können, setzen Cyber-Kriminelle beispielsweise auf Man-in-the-Middle-Konzepte. Dabei stehen Angreifer zwischen den Kommunikationspartnern und erhalten die vollständige Kontrolle über deren Datenverkehr, womit sie Informationen nach Belieben einsehen oder manipulieren können. Die Angreifer täuschen den Kommunikationspartnern dabei vor, das jeweilige Gegenüber zu sein.

Ransomware im PKW

Desweiteren ist der Einsatz von Ransomware (auch Erpresser- oder Verschlüsselungstrojaner genannt) im IoT-Umfeld denkbar. Hier kann es sich um Angriffe handeln, in deren Rahmen ein Opfer innerhalb des eigenen Autos oder in den eigenen vier Wänden getroffen werden kann. Die Folgen solcher Angriffe könnten rasch eskalieren: „Man muss sich vorstellen, was passieren könnte, wenn Ransomware beispielsweise während der Fahrt eines kompromittierten Kraftfahrzeuges aktiv wird und den Fahrer bei hoher Geschwindigkeit nur wenige Sekunden vom Straßenverkehr ablenkt, die Bremse betätigt oder beschleunigt, wenn einer Lösegeldzahlung, beispielsweise durch Erpressung der Kreditkartendaten über eine bestehende Telefonverbindung, nicht umgehend nachgekommen wird", skizziert Raphael Labaca Castro von Eset ein Angriffsszenario. Dies mag zwar surreal klingen, ist mit Verweis auf den Hack eines Fahrzeugs der Marke ‚Jeep' im Sommer 2015 keinesfalls Zukunftsmusik: Hierbei konnten die beteiligten Forscher von der Couch aus viele wichtige Fahrzeugfunktionen steuern, darunter Klimaanlage, Scheibenwischer und eben auch Bremse und Beschleunigung.

Um im Internet der Dinge generell vor Cyber-Angriffen gefeit zu sein, gilt es, Sicherheitsmechanismen bereits bei den ersten Konzepten von IoT-Lösungen zu berücksichtigen. Zwar sei die Verwendung von Firewalls, Virenscanner und Passwörter laut Kügler ein erster Ansatz. Dieser reiche allerdings nicht aus. „Jeder Teilnehmer im Internet der Dinge steht vor zwei Herausforderungen: Er muss sich selber gegen Manipulationen schützen und er muss andere Teilnehmer sicher erkennen. Ein sicherer Schutz gegen eine Veränderung beinhaltet Secure Boot und Verschlüsselung von ausführbarem Code. Zudem erfordert die sichere Erkennung den Einsatz von Zertifikaten", erläutert Kügler. Desweiteren sind Verschlüsselungs- bzw. kryptographische Mechanismen wichtige Kernpunkte der Abwehrmaßnahmen. „Denn neben der Verschlüsselung spielen Einwegfunktionen (Hash) für einen Fingerabdruck, elektronische Unterschriften (Signaturen) und Beglaubigungen (Zertifikate) eine wichtige Rolle", betont Kügler abschließend.

Bildquelle: Thinkstock/Purestock

Zurück

Ähnliche Nachrichten