

Jans Abstract

Marius Abstract

Davids Abstract: Im Bereich Internet of Things hat das Thema Angriff eine besondere Relevanz. IoT Geräte sind meist rund um die Uhr online. Das steigert nicht zuletzt die Attraktivität für Angreifer. Haben Angreifer erst einmal Zugriff auf ein Gerät, so nutzen sie es häufig für DDoS-Attacken. IoT-Geräte einer Baureihe werden bei der Produktion meist alle mit dem gleichen Image bespielt. Dadurch sind die Geräte softwaretechnische alle gleich. Sie haben den gleichen User und dieser hat auch immer das gleiche Passwort. So ist es Angreifern möglich, mit geringem Aufwand Zugriff auf viele Geräte zu erhalten. Ferner kommen oft veraltete Linux-Distributionen bei IoT-Devices zum Einsatz. Diese haben dann dementsprechend viele Sicherheitslücken. Hier ist der Besitzer des Gerätes oft auf den Hersteller angewiesen. Es sollte regelmäßig Updates verteilen. Auch ist es für den Besitzer ratsam, seine IoT-Geräte hinter einer Firewall zu betreiben. Ist die Firewall richtig konfiguriert, so besteht ein effektiver Schutz vor unberechtigtem Zugriff. Im Hinblick auf den Datenschutz sollte man sich auch vor Augen halten, über welche sensiblen Daten die einzelnen IoT-Geräte verfügen. Derartige sensible Daten sind meist für diese Geräte essentiell, sie benötigen sie um zu arbeiten. So muss beispielsweise eine sprachgesteuerte Hausautomatisierung alle Gespräche mithören um ihr Schlüsselwort zu erkennen. Inwiefern die aufgezeichneten Gespräche nun verarbeitet werden, ist nicht immer ersichtlich, sollte die Software nicht quelloffen sein. Ist die Datenverarbeitung ausgelagert, so ist ebenfalls nicht nachvollziehbar was mit den Daten passiert. Nicht auszuschließen ist, dass Anbieter derartiger Lösungen die gesammelten Daten wirtschaftlich nutzen. Ihnen kann es möglich sein, Rückschlüsse auf das Verhalten des Nutzers zu ziehen, wenn sie über die entsprechenden sensiblen Daten verfügen.