IoT - Bedrohungs Phänomene

Ein zentraler Aspekt im Internet of Things ist das Thema Sicherheit: Jedes mit dem Internet verbundene Gerät kann prinzipiell in die Schusslinie von Cyberkriminellen geraten. Hier findest du daher einen Überblick über mögliche Gefahren, von denen Nutzer von IoT-Geräten betroffen sein können.

Man-in-the-middle Angriff

Ein Man-in-the-Middle-Attack ist ein aktiver Abhörangriff, bei dem ein Hacker Nachrichten von einem zum nächsten Opfer weiterleitet. Die Opfer werden somit im Glauben gelassen, dass sie miteinander kommunizieren. Da viele IoT-Produkte mit schlecht konfigurierten Einstellungen auf den Markt kommen, sind diese Geräte leichter für MITM-Angriffe anfällig.

Denial-of-Service Angriff

Ein DoS-Angriff versucht durch eine gezielt herbeigeführte Überlastung die nicht Verfügbarkeit eines Internet-Services herbeizuführen. Meistens steht eine DoS-Attacke dahinter, wenn eine Website durch Hacker unerreichbar gemacht wurde. Diese Methode kann jedoch auch für IoT-Geräte schädlich sein

War Driving

Wardriving ist das systematische Suchen nach offenen oder oftmals schlecht gesicherten Wireless Local Area Netzwerks mit Hilfe eines Fahrzeugs. Ist das Netzwerk gehackt, reicht oftmals nur ein Befehl um alle angeschlossenen Geräte anzeigen zu können

Phishing

Phishing ist ein Kunstwort, das sich aus den Worten „Passwort“ und „fishing“ zusammensetzt. Kriminelle verwenden hier Methoden, um als vertrauenswürdiger Kontakt zu erscheinen und so an wertvolle Informationen zu gelangen.

Eaves Dropping

Eavesdropping Attacken sind Angriffe, die das heimliche Abhören oder Mitlesen von Gesprächen oder Nachrichten zum Ziel haben. IoT Geräte verfügen oftmals nicht über die Rechenleistung oder Energie für verschlüsselten Datenaustausch im Haushalt, wodurch diese oft sehr anfällig für Eavesdropping Attacken sind.

SYNYO GmbH
Research // Development // Advisory

www.iothink.at

SYNYO

netidee FÖRDERUNGEN