SICHERHEIT IM INTERNET DER DINGE

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. Die entsprechenden Tipps helfen dir, diesen Gefahren zu entgehen und einen sicheren Umgang mit IoT-Geräten zu meistern.

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.

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.

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

Tipps für den sicheren Umgang mit dem Internet der Dinge

#1 Username und Passwort regelmäßig ändern

Der Benutzername und das Passwort sollten sofort nach dem Kauf eines Gerätes geändert und danach in regelmäßigen Abständen (ca. alle 3 Monate) upgedatet werden. Ein sicheres Passwort beinhaltet Klein- und Großbuchstaben, Symbole, Zahlen oder eine PIN.

2 Achtung bei Smart Toys!

Smart Toys erkennen ihre Umgebung und reagieren auf Sprachbefehle oder andere Interkationen mit dem Menschen. Spielzeuge, die nicht benutzt werden, sollten stets ausgeschaltet werden. Die Inbetriebnahme sollte überdies nur in einer „sicheren“ Umgebung stattfinden, Standardpasswörter sollten stets geändert werden.

#3 Stets Sichere Netzwerke Verwenden

Das verwendete Netzwerk sollte sicher sein. Dafür sollte WiFi mit starkem Passwort oder VPN benutzt werden. Es sollte überprüft werden, ob der verwendete Router eine Firewall integriert hat und ob diese aktiviert ist. Das dort voreingestellte Passwort sollte laufend geändert und verfügbare Updates eingespielt werden.

#4 Ungesicherte Verbindungen meiden

Da ungesicherte Internet Verbindungen ein großes Risiko für Cyberangriffe darstellen, sollte man nicht über ungesicherte Bluetooth oder WLAN-Verbindungen online gehen. Die Kommunikation mit dem Internet sollte möglichst über HTTPS oder TLS erfolgen.

#5 Wachsamkeit Bei Persönlichen Informationen Im Internet

Es sollte stets darauf geachtet werden, welche Daten von einem IoT-Gerät gesammelt werden. Besondere Wachsamkeit ist bei personenbezogenen Daten geboten – insbesondere dann, wenn diese nicht zur Funktion des Gerätes notwendig sind. Wenn nötig, können auch frei erdachte Informationen verwendet werden.

#6 IoT-Geräte für Kinder

Bei IoT Geräten gibt es Geräte, die auch von Kindern verwendet werden und solche, die speziell für Kinder entwickelt wurden, zum Beispiel Interaktive Spielzeuge. Da solche Geräte stark miteinander vernetzt sind, besteht die Gefahr, dass diese einfach überwacht werden können. Lauschangriffe durch intelligente Spielsachen können ein Risiko darstellen.

#7 Verwendung von 2-Faktor-Authentifizierungsmethode

IoT-Geräte, die nur durch ein Passwort geschützt sind, sind nicht sicher. Durch die Verwendung der 2-Faktor Identifizierungsmethode können sich Nutzer leicht vor Hackerangriffen schützen. Diese ermöglicht den Identitätsnachweis eines Nutzers mittels Kombination zweier unterschiedlicher, unabhängiger Komponenten.

#8 Sicherheitsniveau Beachten

IoT Geräte setzen ein gewisses Maß an Sicherheitsanforderungen voraus, um den Verbraucher zu schützen. Hersteller müssen Datenschutzrichtlinien für IoT-Geräte beachten. Verbraucher sollen durch den Hersteller informiert werden, wie sie die Sicherheitseinstellungen ihrer Geräte anpassen sollen.

#9 Achtung Bei Live Video Streamings

Durch das leichte Uploaden von Videos mit einem Smartphone können ungewollte Inhalte durch Fremde oder Dritte im Internet verbreitet werden. Für mehr Sicherheit und Privatsphäre im Internet auf Sozialen Medien empfiehlt es sich, seinen Aufenthalts- bzw. Wohnort nicht anzugeben.

#10 Frage Jemanden Um Rat, Dem Du Vertraust

Wenn du dich in einer Situation befindest, in der du unsicher oder misstrauisch bist, frage jemanden um Rat dem du vertraust – egal ob Eltern, Freunde oder Lehrer.

SYNYO GmbH
Research // Development // Advisory

www.iothink.at

SYNYO

netidee FÖRDERUNGEN