Die 10 typischen IoT Security-Fehler

1

Schwache, erratbare oder hardcoded Passwörter

Verwendung von leicht erratbaren, öffentlich zugänglichen oder unveränderlichen Anmeldeinformationen wie z. B. fixe Herstellerpasswörter, Default-Servicezugänge.

2

Unsichere Netzwerkdienste

Nicht benötigte oder unsichere Netzwerkdienste, die auf dem Gerät selbst ausgeführt werden, insbesondere solche, die dem Internet ausgesetzt sind, sowie die Vertraulichkeit, Integrität / Authentizität oder Verfügbarkeit von Informationen beeinträchtigen oder eine unbefugte Fernsteuerung ermöglichen.

3

Unsichere IoT-Ökosystem-Schnittstellen

Unsichere Web-, Backend-API-, Cloud- oder mobile Schnittstellen im IoT-Ökosystem ausserhalb des Geräts, die eine Gefährdung des Geräts oder der zugehörigen Komponenten ermöglichen. Häufige Probleme sind ein Mangel an Authentifizierung / Autorisierung, fehlende oder schwache Verschlüsselung und ein Mangel an Ein- und Ausgangsfilterung.

4

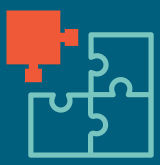
Fehlender sicherer Aktualisierungsmechanismus

Fehlende Möglichkeiten, das Gerät sicher zu aktualisieren. Dazu gehören fehlende Firmware-Validierung auf dem Gerät, mangelnde sichere Bereitstellung (unverschlüsselt während der Übertragung), fehlende Anti-Rollback-Mechanismen und fehlende Benachrichtigungen über Sicherheitsänderungen aufgrund von eingespielten Updates.

5

Verwendung von unsicheren oder veralteten Komponenten

Verwendung von veralteten oder unsicheren Softwarekomponenten / Bibliotheken, die eine Gefährdung des Geräts ermöglichen könnten. Dazu gehört die unsichere Anpassung von Betriebssystemplattformen. Auch die Verwendung von Soft- oder Hardwarekomponenten von Drittanbietern aus einer gefährdeten Lieferkette fällt darunter.



6

Unzureichender Schutz der Privatsphäre

Persönliche Daten des Benutzers, die auf dem Gerät oder im IoT-Ökosystem gespeichert sind und unsicher, unsachgemäss oder ohne Genehmigung verwendet werden.

7

Unsicherer Datentransfer und unsichere Datenspeicherung

Fehlende Verschlüsselung oder Zugriffskontrolle auf sensible Daten innerhalb des gesamten IoT-Ökosystems. Dies betrifft Daten im Ruhezustand, während des Transports oder während der Verarbeitung. Sicheres Protokollieren von Login, Setzen von Einstellungen oder Signieren von erzeugten Daten wie Files und PDF fehlt.

8

Fehlende Geräteverwaltung

Fehlende Sicherheitsunterstützung für Geräte, die in der Produktion eingesetzt werden, einschliesslich Asset-Management, Update-Management, sichere Ausserbetriebnahme, Systemüberwachung und Reaktionsfähigkeiten.

9

Unsichere Standardeinstellungen

Geräte oder Systeme, die mit unsicheren Standardeinstellungen ausgeliefert werden, oder die nicht in der Lage sind, das System sicherer zu machen, indem sie die Bediener daran hindern, Konfigurationen zu ändern.

10

Fehlende physikalische Härtung

Fehlende physische Härtungsmassnahmen, die es potenziellen Angreifern ermöglichen, sensible Informationen zu erhalten, die bei einem zukünftigen Remote-Angriff helfen oder die lokale Kontrolle über das Gerät übernehmen können.

CyOne Security AG
Hinterbergstrasse 18
6312 Steinhausen

Telefon +41 41 748 85 00
info@cyone.ch
cyone.ch

CyOne SECURITY