Smartphones im Produktionsumfeld

Dieses Dokument behandelt nur den Umgang mit Smartphones die ausschließlich im Unternehmen verwendet werden. Für den Privatgebrauch müssen weitere Maßnahmen unternommen werden, die neu auftretenden Problemen entgegenwirken. Auf Bring Your Own Device wird nicht eingegangen.

Bedrohungen

Beim Betrieb von Smartphones im Produktionsumfeld gibt es grundsätzliche Dinge, die man bezüglich Sicherheit beachten muss, vor allem da mit der Industrie 4.0 sehr viele Komponenten der Anlage eine immer höhere Konnektivität aufweisen.

Allgemeine Gefahren

Hinzu kommt, dass die Geräte bei Verlust oder Diebstahl ein Risiko darstellen, da unbefugte Personen leichter an vertrauensvolle Daten kommen können, insbesondere wenn keine Maßnahmen ergriffen werden. Ein signifikanter Punkt ist der Internetzugang, da allein übers Internet schon viele Angriffsmöglichkeiten entstehen und sobald ein Angreifer ins Intranet des Unternehmens gelangt ist, er sich bis zum Produktionsnetz vorarbeiten kann.
Bei Smartphones besteht zusätzlich ein Sicherheitsrisiko, wenn dieses gerootet oder gejailbreakt wird, da so einige Sicherheitsfunktionen außer Kraft gesetzt werden. Dann gibt es wie bei allen anderen Geräten auch folgende Schwachstellen

- unsichere Passwörter
- veraltete Software
- Verlust oder Diebstahl
- falsche Konfiguration

Produktionsbedingte Besonderheiten

Da die Kommunikation des Smartphones mit der Anlage drahtlos erfolgt, besteht an dieser Stelle die Gefahr, dass Hacker die Kommunikation mithören oder sogar manipulieren. Dabei gibt es die Möglichkeit, dass Angreifer die Kommunikation mitschneiden und immer wieder “abspielen”, während sie insgeheim der Anlage andere Steuerungsbefehle zusenden und so lange unbemerkt bleiben können, um Schaden anzurichten.

Sicherheitsmaßnahmen

Am sichersten wäre es Smartphones nicht im Produktionskontext zu verwenden, aber sollte der Nutzen überwiegen, muss man Maßnahmen ergreifen, um sich vor Angriffen zu schützen.
Grundlegendes:

- starke Passwörter
- regelmäßige Updates durchführen
- Internetnutzung deaktivieren
- Multi-Faktor-Authentifizierung
- automatische Bildschirmsperre
- Gerätehärtung
    - nur nötige Software und Features, alles andere löschen/deaktivieren

    - alle Einstellungen so strikt wie möglich konfigurieren

In Bezug auf Anlagensteuerung:

- Benutzerrollen einrichten
- verschlüsselter Zugang zu ICS
- Schutzzonen einrichten
- Black-Channel-Kommunikation (sicherheitsrelevante Daten werden über ein sicheres und isoliertes Netz ausgetauscht)

Mobile Device Management

Für mobile Geräte eignet sich ein Mobile Device Management (MDM). Damit ist es möglich ein Smartphone aus der Ferne zu löschen oder zu sperren. Außerdem vereinfacht es die Datenverwaltung, da sie zentral geregelt wird und einfach überwacht werden kann. Ein MDM verhindert Jailbreaking und Rooting und man kann ein Nutzungsbereich definieren, sodass außerhalb dieses Gebietes das Mobilgerät nicht genutzt werden kann. Man kann regeln welche Apps zum Download zugelassen sind, was von vornherein widerrechtliche Downloads von unsicheren Apps oder die Installation von Apps aus nicht verifizierten Quellen verhindert.
Allerdings müssen Nutzen und Kosten aufgewogen werden, da es aufwendig und kostspielig ist ein MDM zu etablieren.

Biometrische Authentifizierung

Biometrische Authentifizierung, wie Fingerabdruckscanner und Gesichtserkennung, eignet sich nur bedingt, da sie fehleranfällig sind. Es besteht das Risiko, dass falsche Identifikatoren als richtig erkannt werden und richtige als falsch. Somit ist von Authentifizierung allein über biometrische Mittel abzuraten.

Dieses Dokument orientiert sich an:
IEC-62443-2-1 Norm, insbesondere die Komponente SPE4 - Komponentensicherheit: COMP1.1 - Gerätehärtung,
einem Dokument des BSI über Top 10 Bedrohungen und Gegenmaßnahmen für ICS von den Jahren 2021 und 2022
(https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=1),
Dokument des IFA zu "Verwendung von Tablets und Smartphones zur Maschinensteuerung"
(https://publikationen.dguv.de/forschung/ifa/aus-der-arbeit-des-ifa/3390/verwendung-von-tablets-und-smartphones-zur-maschinensteuerung-aus-der-arbeit-des-ifa-nr.-0398),
Dokument von NIST "Guide to ICS Security"
(https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final)