Geräte und Datenträger

Problembeschreibung

Besonders mobile Geräte und Datenträger stellen ein Sicherheitsrisiko für die Produktionslinie eines Unternehmens dar. Was diese Komponenten so anfällig macht, sind vor allem die unterschiedlichen Netzwerke, mit denen die Geräte sich verbinden. Denn über öffentliche und ungesicherte Netzwerke können Schadprogramme auf den Dienstlaptop oder den Firmen-Stick gelangen, welche sich ohne die nötige Vorsicht im Unternehmensnetz oder sogar im Produktionsnetzwerk ausbreiten, sobald sie in Kontakt damit kommen.
Gerade die Gefahr bei Wechseldatenträgern wird unterschätzt. Da ein USB-Stick direkt in den Arbeitsrechner oder in die Anlage gesteckt wird, werden häufig wichtige Sicherheitsmaßnahmen übersprungen, was Angreifern ein leichtes Einfallstor bietet. Ebenso riskant wird die unachtsame Verwendung von Wechseldatenträgern durch den privaten Gebrauch im Heimnetzwerk und die Nutzung von Geräten externer Dienstleister.

Aber auch bei fest installierten Geräten sollte man auf die richtige Handhabung achten, denn schnell kann Schadcode durch nicht regelmäßig gewartete Software in das Unternehmensnetz eindringen. Gerade wenn die Software nicht benötigt wird, gerät sie schnell in Vergessenheit und wird nicht auf dem aktuellsten und somit sichersten Stand gehalten.

Gefahren

Ist Malware erst einmal eingedrungen kann es zu mehreren möglichen Schäden führen. Problematisch dabei ist, dass Malware nur selten sofort erkannt wird, sodass ein Angreifer über einen längeren Zeitraum Zugang zum System haben kann. Dabei entstehende Risiken und Angriffsformen sind meist eine der Folgenden:

- Beeinträchtigung oder Lahmlegung der Produktionslinie
- Fernspionage und Sammeln vertraulicher Informationen
- Verschlüsselung von wichtigen Daten und Erpressung

Sicherheitsmaßnahmen

Um die oben beschriebenen Gefahren zu vermeiden, ist es erforderlich einen Standard von Sicherheitsmaßnahmen zu etablieren.

Geräte

- Jedes verwendete Gerät sollte vor oder während der Installation gehärtet werden.
    - Löschen oder Deaktivieren nicht benötigter Software
    - Deaktivieren nicht benötigter Netzwerkschnittstellen

    - Netzwerkports physisch oder logisch sichern
    - strikte Konfiguration bezüglich Zugriffsrechten
    - so wenig drahtlose Schnittstellen wie möglich
    - nur autorisierte Änderungen der Konfiguration zulassen
    - physische Schlösser gegen unbefugtes Anschließen am Gerät anbringen
- Einen Prozess etablieren, der die Gerätehärtung aufrecht erhält.

Datenträger

- vor dem Gebrauch auf Schadcode prüfen
    - Virenscanner verwenden
    - Isoliertes Netz bzw. gesonderten Rechner für Prüfung verwenden
- sofern möglich Datenträger ausschließlich im Unternehmensnetzwerk nutzen
- niemals unbekannte Datenträger verwenden
- erhaltene Datenträger zusätzlich vom Lieferanten absichern lassen
    - Digitale Signatur (Überprüfung ob das erhaltene Programm dem unverfälschten vom Hersteller entspricht)
    - Antimanipulationssiegel (Änderungen des Datenträgers werden erkannt und gemeldet)
- Whitelisting (nur zur Verwendung freigegebene Datenträger erhalten Lese- und Schreibrechte, alle anderen werden direkt vom System abgelehnt)
- die Autorun-Funktion deaktivieren, damit nicht Programme direkt beim Einstecken ausgeführt werden
- Datenträger verschlüsseln

Dieses Dokument orientiert sich an der IEC-62443-2-1 Norm, insbesondere die Komponente 9.2 COMP 1 - Geräte und Datenträger, einem Dokument des BSI über Top 10 Bedrohungen und Gegenmaßnahmen für ICS (https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=1), sowie eines Artikels über USB-Sticks im industriellen Umfeld von stromshield (https://www.stormshield.com/de/news/das-paradox-des-usb-sticks-im-industriellen-bereich/)