SafeWise
17.06.2022

Modul 2: Erweiterung der Cyber-Sicherheit

Fernzugriff (SPS)

Mit Fernzugriff ist ein Zugriff auf IT-Systeme und die darauf laufenden Anlagen und Anwendungen von außerhalb des Netzwerkes gemeint.
Dieser Zugriff kann genutzt werden, um auf Firmeninterne Daten, Anwendungen, Geräte und Anlagen zuzugreifen und Änderungen durchzuführen ohne Vorort zu sein.
Hier ist es unglaublich wichtig, sich an die Vorgaben und Richtlinien des Arbeitgebers zu halten, da es sich z.B. im Falle der SPS um einen direkten Zugang auf das Herzstück des Unternehmens handeln kann.

Folgende Punkte musst du beachten:

- Regeln beim Einrichten des Fernzugriffs beachten
    - nur sichere Kommunikationsprotokolle, Verschlüsselungsalgorithmen oder Authentisierungsmechanismen einsetzen
    - sichere und lange Passwörter verwenden
    - Regelmäßige und professionelle Wartung
    - Bei Wartung durch Dritte
        - Vertragliche Grundlage erstellen
            - regelt Rollentrennungen usw.
- Bei Nutzung von Online-Diensten (Browser) zum Aufrufen des Fernzugriffs darauf achten, das Ende-zu-Ende verschlüsselt wird.

Netzwerksegmentierung

Netzwerksegmentierung ist ein Netzwerksicherheitsverfahren, bei welchem ein Netzwerk in kleinere, separate Subnetzwerke unterteilt wird.

Ein ICS-Netz (industrielle Kontrollsystem) sollte aus mehrere kleinen Netzwerken mit verschiedenem Schutzbedarf bestehen.
Datenaustausch zwischen den verschiedenen Leveln des ICS sollten durch eine Datenflusskontrolle verlaufen (Firewall).

Bei hohem Schutzbedarf sollte zwischen Produktionsführung und der Betriebs-/Prozessführung eine demilitarisierte Zone (DMZ) eingerichtet werden. Diese ist ein Zwischennetz, das zwischen zwei Netze geschaltet wird, aber zu keinem der beiden Netze gehört.
Die DMZ ist ein eigenes Netz, das nicht so stark gesichert wird wie das zu schützende Netz. Es besteht aus zwei physisch getrennten Firewalls und einem Application Level Gateway. Hier wird der Datenverkehr mittels Proxydiensten mit Filtermöglichkeiten bis hin zum Layer 7 gesteuert und kontrolliert.

Netze sollten anhand ihrer Funktionalitäten getrennt werden (vertikale Integration).
Des Weiteren sollte auch standortübergreifende Netze und allgemein organisatorisch unabhängige Maschinen/Anlagen segmentiert werden (horizontale Integration).
Da sich die Schadprogramme sonst auf alle Maschinen ausbreiten.

Verbindungsaufbau sollte immer vom Netzsegment mit höherem Schutzbedarf zum Netzsegment mit niedrigerem Schutzbedarf gehen.

Eine undokumentierte Verbindung und eine dadurch umgangene Netztrennung sollte niemals stattfinden.

Quellen:

Fernzugriff (SPS)

- OPS.1.2.5 Fernwartung
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_2_5_Fernwartung_Edition_2022.pdf?__blob=publicationFile&v=3

Netzwerksegmentierung

- BSI ICS Kompendium
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=3