MAXXYS.

IT-SECURITY KONZEPT INDUSTRIE 4.0

HERAUSFORDERUNGEN

Im Rahmen von Industrie 4.0 nimmt die Vernetzung von Maschinen und Anlagen drastisch zu. Automatisierungs-, Prozesssteuerungs- und Prozessleitsysteme werden heute in nahezu allen Produktionsanlagen und Produktionsnetzen eingesetzt.

Während die Fertigungs- und Produktionsanlagen (Industrial Control System => ICS) früher weitgehend abgeschirmt waren und autonom liefen, sind sie heute hochgradig mit der Unternehmens-IT und dem Internet vernetzt und damit denselben Cyber-Angriffen ausgesetzt, wie in der konventionellen IT-Umgebung.

Die Herausforderungen in puncto Sicherheit steigen somit enorm..

MAXXYS.

Aufgrund existierender Schwachstellen in den Fertigungs- und Produktionsanlagen (ICS) resultieren Cyber-Angriffe, welche den industriellen Anlagen und dem gesamten Unternehmen großen Schaden zufügen können.
Es gilt Schnittstellen und Sicherheitslücken zu schließen, um eine sichere Kommunikation in stark vernetzten Systemen zu gewährleisten.

Zu den häufigsten Angriffen zählen:

- Social Engineering und Phising
- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über das Internet
- Einbruch durch Fernwartungszugängen
- Menschliches Fehlverhalten und Sabotage
- Internet verbundene Steuerungskomponenten
- Technisches Fehlverhalten D)DoS Angriffe

SCHRITT 1
Bestandsaufnahme und Analyse der IT-Infrastruktur des Unternehmens und der Produktionsanlagen:

- welche Plattformen und Systeme werden eingesetzt
- welche Sicherheitsmaßnahmen / Softwarelösungen sind bereits im Einsatz, um die Sicherheit aller Produktionsanlagen zu gewährleisten
- wie funktioniert die sicherheitstechnische Vernetzung / Zusammenspiel der Systeme zur Fertigungs- und Prozessautomatisierung untereinander und mit der klassischen IT-Infrastruktur

SCHRITT 2
Betrachtung und Beurteilung des IT-Sicherheitsniveaus im Unternehmen und Produktionsnetz:

- Erkennen und Einschätzen von Bedrohungen im Produktionsnetz
- Identifizierung von Schwachstellen und Bewertung des Risikoausmaßes
- Verfügbarkeitsanforderungen von Kommunikationsnetzen und deren Überwachung analysieren und dokumentieren

SCHRITT 3
Beurteilung des Gefährdungspotentials auf Basis von:

- menschlichem Fehlverhalten
- vorsätzlichen Angriffen auf Geräte-, Netz- und Anwendungsebene
- Vernetzungsgrad und Absicherung der Produktionsnetze und der Unternehmens-IT
- Fehlkonfigurationen, fehlende Softwareupdates und unzureichende Backups von Komponenten
- passive und aktive Angriffe auf etablierte ICS-Komponenten wie SCADA-Systeme, PLC, HMI, BFS und MES auf System- und Netzwerkebene

MAXXYS.

SCHRITT 4
Ganzheitliche IT-Infrastruktur in und für die Unternehmens-IT und die industrielle Systemsteuerung (ICS)

Security Awareness

- Sensibilisierung von Mitarbeitern/innen
- Sicherheitskampagnen: Zielgruppen- und ereignisgesteuert Stärkung der „Human Firewall“

Schnittstellenkontrolle

- Richtlinie, wer welche Dateien lesen und/oder kopieren darf
- Kontrolle, wer zu welchem Zeitpunkt welche Datei auf welches Medium kopiert (z. B. keine EXE-Dateien auf Share)
- Kontrolle von Netzwerklaufwerken und externen Laufwerken, wer zu welchem Zeitpunkt welches Laufwerk verwenden darf
- Richtlinie, welche Dateien wohin kopiert werden dürfen

Verschlüsselung von Daten

- Sichere Dateiverschlüsselung in der Cloud, auf Servern, Desktops und Laptops
- Verschlüsselung externer Laufwerke wie USB-Sticks
- Benutzer- und gruppenbasierte Zugriffsberechtigungen
- Zentrales Schlüsselmanagement mit Self-Service-Funktion zur Aufstellung von Benutzerschlüsseln
- Integriertes zentrales Reporting mit umfassenden Analysemöglichkeiten
- Encryption 2-Go

Applikationskontrollen

- Nicht genehmigte Programme werden gestoppt, bevor sie Schaden anrichten können
- Verhindert Zero-Day Exploits
- Festgelegte Regeln bleiben nach Software Upgrades bestehen
- Transparentes und effizientes Black- an Whitelisting

MAXXYS.

SCHRITT 4

Ganzheitliche IT-Infrastruktur in und für die Unternehmens-IT und die industrielle Systemsteuerung (ICS)

Endpunktmanagement

- automatisierte Softwareverteilung
- flexiblen und automatische Installationsverfahren von Software und Betriebssystemen
- Automatisches, manuelles, regelbasiertes und sicheres Patchmanagement
- Automatisierte Verwaltung von mobilen Endgeräten

Identitäts- und Zugriffsmanagement

- Identitätsverwaltung, On- und Offboarding
- Bereinigung von Berechtigungen, Zertifizierungen, Aufgabentrennungen und Rollenmanagement
- Automatisierung und Verwaltung von identitätsbezogenen Workflows
- Provisionierung/Deprovisionierung, Anwender-Self-Service
- Auditing und Reporting im Hinblick auf die Compliance Unterstützung bei der Einführung einheitlicher Security-Richtlinien für Identitäten => Richtlinienmanagement
- die Vereinfachung der Compliance und die Automatisierung wichtiger Prozesse
- => Workflow Management

Zugriffsmanagement von privilegierten Anwendern und externen Dienstleistern

- Transparenz und Management von Zugriffen nicht nur privilegierter Accounts
- Passwortmanagement und Session-Aufzeichnung
- Kontrolle der Aktivitäten privilegierter Nutzer für Compliance-Zwecke

Programmierschnittstellen (APIs) verwalten

- Veröffentlichung, Optimierung und Kontrolle von Programmierschnittstellen
- Integration von Sicherheitsrichtlinien

Der Einsatz der richtigen Software Lösungen, ein dauerhafter Prozess, sowie langjähriges Know-how zur Einbettung von IT-Lösungen in den Gesamtkontext sind notwendig, damit die Unternehmens-IT sicher und reibungslos funktioniert. Wir helfen Unternehmen diesen Prozess zu verstehen und umzusetzen.

MAXXYS.

MAXXYS AG
Am Helgenhaus 15 - 17, 35510 Butzbach

TELEFON
06441 21004 0

EMAIL
info@maxxys.de

Kontaktieren Sie uns!