ANTARES NETLOGIX

FACTSHEET

OT-Security im Automations- und Produktionsumfeld

INDUSTRIAL SECURITY IM KONTEXT VON NIS2

Unter dem Schlagwort „Industrie 4.0" wird die Digitalisierung und somit vor allem die Steuerung, Messbarkeit und Kommerzialisierung in der Produktion vorangetrieben. Das Ziel ist die „intelligente Fabrik" - mit allen Vorteilen und Risiken. Das Gebot der Stunde ist der Blick auf die Sicherheit der Systeme und das Zusammenwachsen der Betriebstechnologie (OT) mit dem Internet. **Nicht die Schnellsten werden überleben, sondern die Sichersten!**

GESCHÄFTSRISIKEN

TOP 5 für Industrieunternehmen*

Die Verschmelzung der physischen und digitalen Welten erhöht die **Abhängigkeit von Technologien** und zunehmend ausgefeilten **Fertigungsprozessen** und bringt dadurch neue operative, sicherheitstechnische und strategische Risiken für Unternehmen mit sich.

Auf der einen Seite steht eine stärker individualisierte, effizientere, robustere und sicherere Produktion, auf der anderen eine **höhere Anfälligkeit für Cyberangriffe und Infrastrukturausfälle in einer extrem vernetzten Welt.**

CYBERVORFÄLLE

Cyberkriminalität, IT-Ausfälle , Geldbußen, Verletzung der Datenschutzrechte

BETRIEBSUNTERBRECHUNG

inkl. Lieferkettenunterbrechung

NATURKATASTROPHEN

Sturm, Überschwemmung, Erdbeben

MAKROÖKONOMISCHE ENTWICKLUNGEN

Inflation, Deflation, Geldpolitik, Sparprogramme

RECHTLICHE VERÄNDERUNGEN

Handelskriege & Zölle, Wirtschaftssanktionen, Protektionismus, Zerfall der Euro-Zone, Brexit

*Quelle: Allianz Risk Barometer

INDUSTRIE IST NICHT GLEICH FABRIK

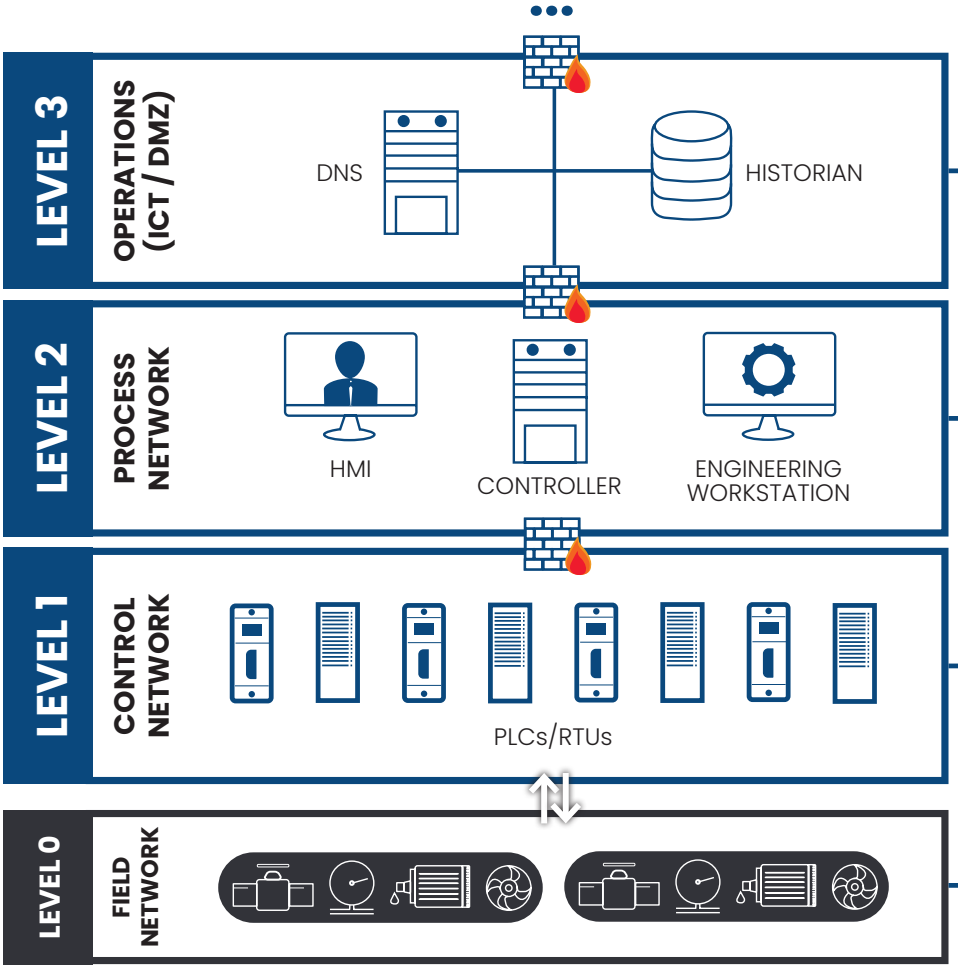
Jede Unternehmensgröße und Branche hat eigene Anforderungen. Manche Gefahren sind jedoch überall latent vorhanden:

- **UNVERSCHLÜSSELTE** Netzwerkprotokolle.
- Veraltete IT-Konzepte: Flache Netzwerke **OHNE SEGMENTIERUNG**.
- Geteilte **PASSWÖRTER** und fehlende **ZWEI-FAKTOR-AUTHENTIFIZIERUNG**.
- Durch eine **CYBERATTACKE** werden **DATEN GELÖSCHT** oder **GESTOHLEN** und die Folgen verschwiegen.
- **WARTUNGSZUGÄNGE** sind intransparent und **ADMIN-ZUGRIFFE** unbeschränkt.

SO **FUNKTIONIERT'S**

OT-Sicherheitskonzepte von Antares-NetlogiX

Produktionsunternehmen sind vom einwandfreien Funktionieren der eingesetzten Betriebstechnologie (OT) abhängig. Mit der vermehrten Abhängigkeit erhöht sich auch der potenzielle Schaden bei einem Ausfall der Systeme. **Schützen Sie Ihre OT gegen unerlaubte Zugriffe und Manipulation von außen und verbessern Sie die Sicherheit!**



UNSERE LEISTUNGEN

- OT SOC
- sichere PKI
- OT Firewall
- Netzwerksegmentierung
- Priviledged Access Managment
- Multi-Faktor-Authentifizierung
- Schwachstellen-Analyse
- Protokollierung
- Alarmierung

NEXT GENERATION SIEM „MADE IN AUSTRIA"

OT SIEM mit der iQSol LogApp

iQSol
Security made in Austria.

Ein **zentrales Log Management** bildet die Grundlage, um viele Anforderungen der NIS2-Richtlinie zu erfüllen und ist gleichzeitig die Basis für ein **modernes OT SIEM.** Dafür gibt es die intelligente iQSol LogApp. Mit dieser Appliance haben Sie jederzeit den Überblick, eine einfache Verwaltung und umfassende Reporting-Funktionen ermöglichen die mühelose Überwachung und Auswertung zahlreicher Log-Quellen. **Die LogApp ist eine zuverlässige OT-SIEM-Plattform „Made in Austria",** mit der Sie die NIS2-Vorgaben sowie andere gesetzliche Bestimmungen problemlos umsetzen können. Die Lösung kann on premise verwendet werden und wird oft auch als isolierte Umgebung für die Protokollierung (und Forensik) eingesetzt.

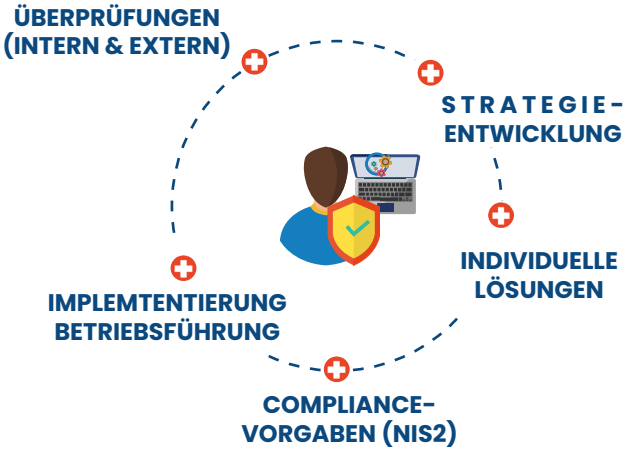
„iQSol macht es möglich: Die LogApp bringt SIEM und Log Management erfolgreich in die OT. Mit den cleveren iQSol-Lösungen sind außerdem Compliance und Business Continuity immer gewährleistet."

DI Alexander Graf, ANLX Geschäftsführer & Certified OT Security Practitioner (COSP)

OT-SICHERHEIT

für Industrieunternehmen

Produktionssysteme laufen nur noch selten in isolierten Umgebungen, denn eine **Verbindung zwischen IT und OT** ist aus vielen Gründen erforderlich. Große Datenmengen verlassen die Fabrikshallen und werden in der Cloud verarbeitet, gespeichert und verändert. Schnittstellen, Medienbrüche und unzählige Geräte sind involviert, wenn es um **neue Geschäftsmodelle, schnellere Kundenbeziehungen und neue Analysemöglichkeiten** geht. Somit ist klar, dass auch bei der Analyse der Logs und Dateien eine **automatisierte Lösung** notwendig ist.



WIR UNTERSTÜTZEN SIE BEI IHREM **INDIVIDUELLEN SICHERHEITSKONZEPT** FÜR **PRODUKTIONSUMGEBUNGEN**!

UNSERE **SICHERHEITSKONZEPTE**

technische Sicherheitsmaßnahmen, Trainings und Workshops

OT-NETZWERKE
- Netzwerksegmentierung innerhalb der OT als Schutz gegen die Ausbreitung von Viren
- Gesicherte Kommunikation zwischen Informationstechnologie (IT) und Betriebstechnologie (OT)

ALARM MANAGEMENT
- Meldung bei Sicherheitsverletzungen und Anlagenstörungen
- Verarbeitung von Störungen aus Anlagen-visualisierungen und PLC-Systemen
- Eskalationsmanagement

NETZWERKMANAGEMENT LAN und WLAN
- Event- & Performance Monitoring
- Rechteverwaltung

NOTFALLMANAGEMENT
- Notfallhandbuch
- Incident Response Team

MANAGED SERVICE
- Antares Operations Center 9x5 oder 24x7
- Betriebsführung Security und Netzwerk
- Übernahme der Wartung und Monitoring

FERNWARTUNGSZUGÄNGE
- SSL / Zwei-Faktor-Authentifizierung
- Privileged Access Management: Zentrales Management und Überwachung der Wartungszugänge für Service-Techniker (intern & extern)

IT-SECURITY MECHANISMEN
- Erkennen von sicherheitskritischen Ereignissen (Angriffe, Viren, unautorisierte Zugriffe)
- Network Access Control (NAC)
- Logging der Aktivitäten im Netz
- Schwachstellen-Assessment & Management

TRAININGS & WORKSHOPS
- Awareness Trainings
- Netzwerktechnik-Trainings

BUSINESS CONTINUITY MANAGEMENT
- Automatisierter Shutdown und Wiederanlauf der Anlagen

COMPLIANCE VORGABEN
- IEC62443, ISO 27001, NIS2 und KRITIS
- IT-Grundschutz (BSI)

OT-MODULE

Mit unseren Modulen sind Sie perfekt vorbereitet!

Unsere Erfahrungen aus vielen Pentests und Sicherheitsaudits im Industrieumfeld zeigen, dass in der Produktion viel **Aufholbedarf in technologischer Hinsicht** besteht. Oftmals sind aber Ansätze und Produkte aus der IT nicht einsetzbar, weil alte Systeme und Geräte vorherrschen. Somit gilt es, individuelle Anforderungen und Notwendigkeiten zu berücksichtigen und in moderne OT-Security-Systeme zu integrieren. So lässt sich auch eine **gute Basissicherheit für IoT-Anwendungen sowie Produktions-, Kassen- oder Robotersysteme** rasch herstellen.

MODUL I

BEST PRACTICE WORKSHOP

- Vorstellung von OT-Sicherheitsstandards und Methoden
- Diskussion der bestehenden OT-Sicherheitsvorkehrungen im Produktionsumfeld (technisch & organisatorisch)
- Erfahrungsberichte aus vergleichbaren Unternehmen
- GAP-Analyse
- Maßnahmenkatalog mit taktischen und strategischen Empfehlungen zur Verbesserung der OT-Sicherheit

MODUL II

PENETRATIONSTEST INDUSTRIE

Wir überprüfen den Zugangsschutz und die Konfigurationsschwachstellen der Anbindung des SCADA/ICS-Netzwerks. Außerdem führen wir in Abstimmung Angriffe auf Server-, Netzwerk- und Feldkomponenten durch und versuchen physikalischen Zugriff zu erlangen.

Aufgrund der großen Verfügbarkeitsproblematik in Produktionsumgebungen erfolgt ein Penetrationstest nur in engster Abstimmung mit dem Kunden!

MODUL III

OT SOC (Security Operations Center)

- Aufbau einer zentralen Appliance, die alle Logs in der OT-Umgebung sammelt
- Anbindung der Steuerungs- und Netzwerkkomponenten
- Aufbau und Integration eines Intrusion Detection Systems
- 24/7 OT-Security Alarmierung durch Cyber Security Analysten

MODUL IV

REIFEGRADANALYSE

- Gap-Analyse: Ist-Situation vs. Compliance-Vorgaben (ICE62443, ISO27001, IT-Grundschutz, NIS2, KRITIS)
- Erarbeitung von Lösungsansätzen bei Abweichungen zu den Compliance-Vorgaben
- Erstellung von Gap-Reports

ANTARES NETLOGIX

Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at

30.10.2024