ANTARES NETLOGIX

FACTSHEET

IT-Security im Automations- und Produktionsumfeld

INDUSTRIAL SECURITY

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 Netzwerke aus verschiedenen Welten. **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.**

1. Cybervorfälle
Cyberkriminalität, IT-Ausfälle , Geldbußen, Verletzung der Datenschutzrechte

2. Betriebsunterbrechung
inkl. Lieferkettenunterbrechung

3. Naturkatastrophen
Sturm, Überschwemmung, Erdbeben

4. Ausbruch einer Pandemie
Gesundheits- & Arbeitskräfteprobleme

5. Rechtliche Veränderungen
Handelskriege & Zölle, Wirtschaftssanktionen, Protektionismus, Zerfall der Euro-Zone, Brexit

INDUSTRIE IST NICHT GLEICH FABRIK

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

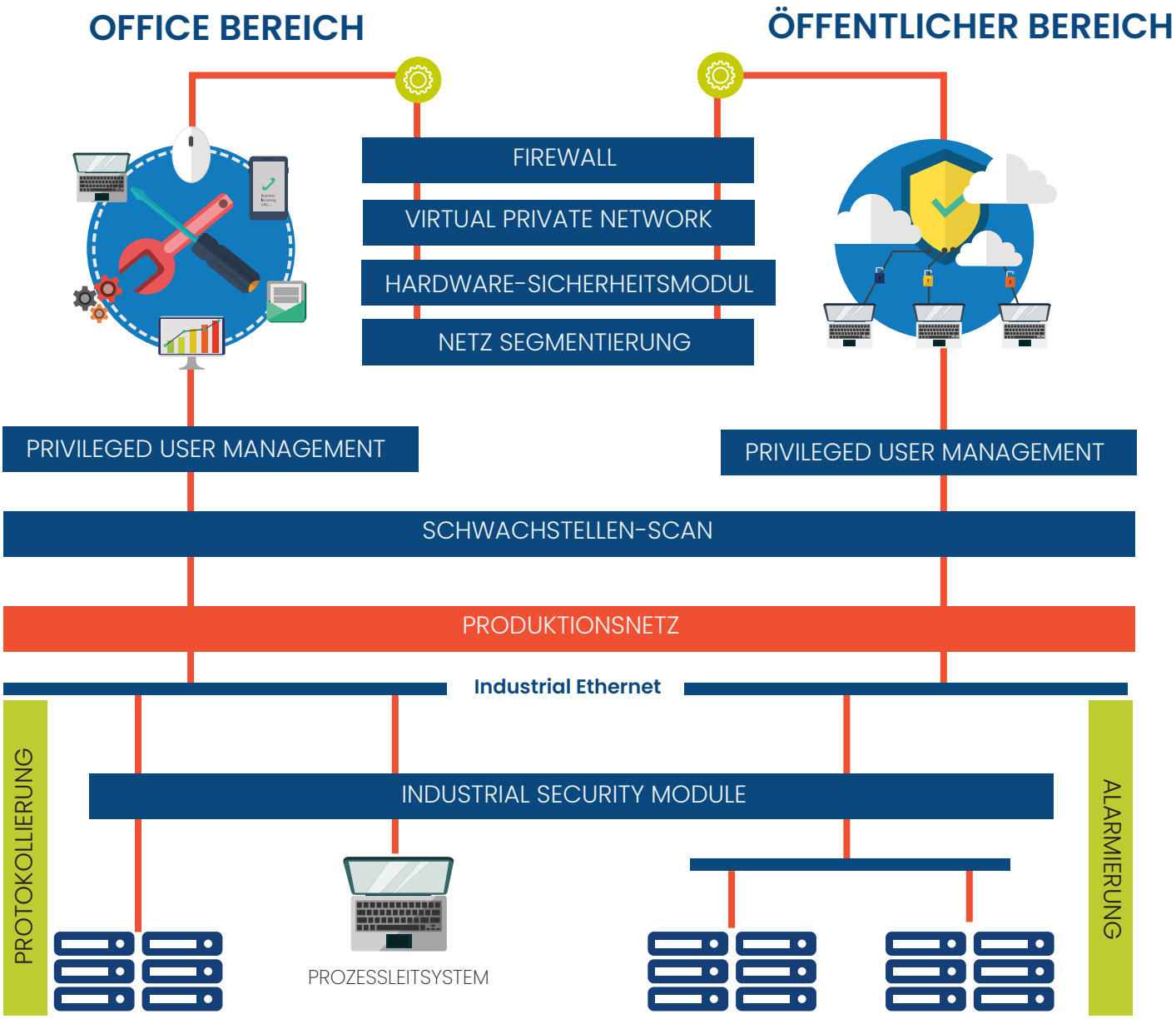
- **USB-STICKS** der Mitarbeiter „**SHAREN**" Informationen aller Art.
- **FREMDE** nutzen **NETZWERKANSCHLÜSSE** und das unsichere **WLAN**.
- **PASSWÖRTER** werden „ausprobiert" und an Dritte weitergegeben.
- **DATEN** werden irrtümlich **GELÖSCHT** und die Folgen verschwiegen.
- **WARTUNGSZUGÄNGE** sind intransparent und **GÄSTEZUGRIFFE** unbeschränkt.

*Quelle: Allilanz Risk Baromenter
https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf

SO **FUNKTIONIERT'S**

IT-Sicherheitskonzepte von Antares-NetlogiX

Produktionsunternehmen sind vom einwandfreien Funktionieren der eingesetzten Informationstechnik (IT) abhängig. Mit der vermehrten Abhängigkeit erhöht sich auch der potenzielle soziale Schaden bei eventuellem Ausfall der Systeme. **Schützen Sie die von der IT verarbeiteten Daten und Informationen und verbessern Sie die Sicherheit!**



EVALUIERUNG & STRATEGIEENTWICKLUNG

IMPLEMENTIERUNG UND BETRIEBSFÜHRUNG

INTERNE UND EXTERNE SECURITY-ÜBERPRÜFUNGEN

AUSARBEITUNG VON INDIVIDUALLÖSUNGEN

COMPLIANCE-VORGABEN

IT-SICHERHEIT

für Industrieunternehmen

Produktionssysteme laufen nur noch selten in isolierten Umgebungen, denn eine **Verbindung zwischen Office- und Produktionswelt** 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

VIRTUAL AUTOMATION NETWORKS
- Netzwerksegmentierung als Schutz gegen die Ausbreitung von Viren
- Gesicherte Kommunikation zwischen Office und Steuerungs- bzw. Leitrechner und Server Netzwerken

ALARM MANAGEMENT
- Meldung bei Sicherheitsverletzungen und Anlagenstörungen
- Verarbeitung von Störungen aus Anlagenvisualisierungen und SPS-Systemen
- Eskalationsmanagement

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

NOTFALLMANAGEMENT
- Notfallhandbuch
- Incident Response Team

MANAGED SERVICE
- Antares Help Desk 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 Training
- Technische Trainings

BUSINESS CONTINUITY MANAGEMENT
- Automatisierter Shutdown und Wiederanlauf der Anlagen

COMPLIANCE VORGABEN
- IEC62443 und ISO 27001
- IT-Grundschutz (BSI)
- EU-Datenschutz-Grundverordnung

SCADA BUNDLES

Mit unseren Bundles 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 IT-Security-Systeme zu integrieren. So lässt sich auch eine **gute Basissicherheit für IoT-Anwendungen sowie Produktions-, Kassen- oder Robotersysteme** rasch herstellen.

BUNDLE I

BEST PRACTICE WORKSHOP

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

BUNDLE 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!

BUNDLE III

TECHNISCHE TEILAUTOMATISIERTE SICHERHEITS-BESTANDSAUFNAHME

- Aufbau einer temporären Monitoring-Infrastruktur (Logging & Schwachstellen-Scan)
- Events werden 30 Tage gesammelt
- Abschlussbericht erkannter Schwachstellen und Angriffsvektoren bzw. ggf. erkannter Vorfälle
- Präsentation und Diskussion des Berichts mit den verantwortlichen Personen

BUNDLE IV

REIFEGRADANALYSE

- Gap-Analyse: Ist-Situation vs. Compliance-Vorgaben
  (ICE62443, ISO27001, IT Grundschutz, EU-Datenschutz-Grundverordnung)
- 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

6 02 2024