TRIOVEGA
SECURELY SHAPING YOUR FUTURE

Produktions-sicherheit und -effizienz

NIS-2 ready!

Mit edge.SHIELDOR OT-Infrastrukturen optimal schützen und Datenkonnektivität zu Ihrem Vorteil nutzen

Ihre Vorteile auf einen Blick

1. Sie härten Ihre OT-Infrastruktur zum effektiven Schutz vor Cyber-Bedrohungen
2. Sie reduzieren Ihr CAPEX und lassen Ihre Maschinen softwareseitig länger laufen
3. Sie sparen Ausgaben bei Maßnahmen zur Mitigierung von Sicherheitsrisiken
4. Sie setzen einen Teil der gesetzlichen Cyber-Sicherheitsvorgaben effizient um
5. Sie bauen operative Exzellenz auf, indem Sie eigene Daten nutzen, um Produktions-effizienzen zu steigern

Der Status Quo an OT-Security Maßnahmen reicht nicht mehr aus

Traditionell schützen Firewalls, Segmentierung und Assetmanagement OT-Netzwerke. Idealerweise sollten alle drei Mechanismen kombiniert werden. Dennoch zeigen Angriffe auf Unternehmen verschiedener Branchen und Größen, dass diese Ansätze nicht mehr ausreichen, um umfassend vor Cyber-Angriffen zu schützen.

Aber warum?

- Weil verfügbare Software-Updates nicht ohne erhebliche Änderungen an den Maschinen in Verbindung mit hohen Mehrkosten ausgerollt werden können.
- Weil für alte Maschinen anbieterseitig oftmals gar keine Software-Updates mehr zur Verfügung gestellt werden.
- Weil notwendige Services wie VPN und Dateiaustausch dafür sorgen, dass Ports manuell geöffnet und nicht alle immer wieder geschlossen werden. Das bestehende Sicherheitskonzept wird so kompromittiert und Netzwerke kommen schnell einem löchrigen Käse gleich.
- Weil Altanlagen oftmals ausschließlich, wenn überhaupt, über unsichere Protokolle kommunizieren und die Schnittstellen nicht homogenisiert sind.

80%
der Unternehmen wurden Opfer eines Cyberangriffs

47%
der Attacken hatten Auswirkungen auf die Betriebstechnik (OT) und Steuerungssysteme (ICS)

NIS-2
Die Umsetzung dieser EU-Richtlinie zur Abwehr von Cyber-Angriffen in nationales Recht muss bereits bis zum **17.10.2024** erfolgen. Verstöße gegen diese Vorgabe können für Unternehmen zu erheblichen Bußgeldern führen.

*Studie „The Global State of Industrial Cybersecurity“ (Claroty), 2023

Resilienz für OT-Infrastrukturen aufbauen

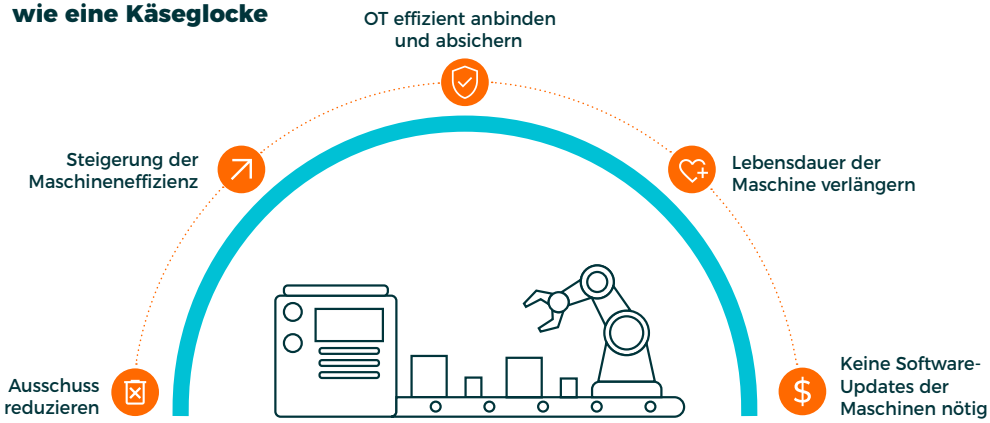
In produzierenden Unternehmen stehen Effizienz und Cyber-Sicherheit in einem Spannungsfeld. Der sicherste Betrieb einer Anlage ist der Offline-Modus, welcher aber jegliche Industrie 4.0 Maßnahmen verwehrt. Um jedoch beides zu erreichen, suchen Unternehmen die Balance zwischen diesen gegensätzlichen Zielen, was immer einen Kompromiss darstellt.

Das optimale Szenario beschreibt in der Industrie:

- Zuverlässiger Schutz vor Cyber-Angriffen
- Erfüllung normativer Anforderungen wie z. B. NIS-2
- Umsetzung effektiver Maßnahmen zur CAPEX- und OPEX-Reduktion
- Produktionseffizienz und -qualität nachhaltig zu steigern

Der edge.SHIELDOR vereint das effiziente Erreichen der gegensätzlichen Ziele von Cybersicherheit und Anlagen-Konnektivität. Um einen sicheren Betrieb der Produktion zu ermöglichen, trennt er jede Anlage im OT-Netzwerk effektiv vom IT-Netzwerk. Sinnbildlich wird über jede Anlage eine Käseglocke gestülpt und schützt so vor Angreifern bei gleichzeitiger Datentransparenz. Ein zentrales Management ermöglicht das einfache Aktualisieren und Härten der Käseglocken, ohne den laufenden Produktionsbetrieb zu unterbrechen oder auf Wartungsfenster angewiesen zu sein.

Das Prinzip ist so einfach wie eine Käseglocke



OT-Security härten und direkten Einfluss auf die Bottom-Line nehmen

Vermeiden Sie unnötige Ausgaben für Software-Updates, softwarebedingte Nachrüstungen oder Neuanschaffungen von Maschinen. Stellen Sie eine sichere Datenkonnektivität über Ihre gesamten Anlagen für Produktionsautomatisierung und datengetriebene Produktionsoptimierung her.

Einfach, sicher, planbar …
Protokollumwandlungen z. B. auf OPC-UA ermöglichen die nahtlose Integration alter und neuer Anlagen, verlängert die Lebensdauer. Unsere Lösung ermöglicht eine sichere Fernwartung. Das zentrale Management sorgt kontinuierlich für die Aktualität der Software, integriert neue Funktionen und stellt sicher, dass der edge.SHIELDOR eine zuverlässige und flexibel anpassbare Lösung für die sich wandelnden Anforderungen der Industrie bleibt.

… und kosteneffizient!
Diese deutliche Verringerung des Verwaltungsaufwandes und das zentrale Management für OT-Netzwerke ermöglichen eine bis zu 80%ige Reduktion der Gesamtkosten für die Maßnahmen der OT-Sicherheitsrisikominderung.

Ihre Vorteile mit edge.SHIELDOR

- **Erhöhte Sicherheit**
- **CAPEX Reduktion**
- **OPEX Einsparungen**
- **Operational Excellence**

Sie fragen sich, wie Sie von edge.SHIELDOR profitieren können? Ich helfe Ihnen gerne weiter!

René Janz
Director Business Development
rja@triovega.com

TRIOVEGA
SECURELY SHAPING YOUR FUTURE

Securely shaping your future

Triovega ist Mitglied der Unternehmensgruppe Viega Holding GmbH & Co. KG. Wir erbringen für unsere Kunden Wertschöpfung im Dienstleistungs-, Projekt- und Produktbereich. Dabei sind wir internationaler Partner in der technischen Beratung, Umsetzung und Qualitätssicherung für Digitalisierungsvorhaben. In enger Kooperation mit erfahrenen und spezialisierten Partnern liefern wir seit 1999 schlüsselfertige Produkte und gefragte Services: von der Planung über die Durchführung bis zur Modernisierung und dem After-Sales Service inkl. begleitender Beratungsdienstleistungen. An den Standorten in Lübeck und Braunschweig entwickeln wir Softwarelösungen und Services für namhafte Industrieunternehmen. Dafür entwickelt unser internationales Team individuelle Konzepte und Dienstleistungen für Herausforderungen rund um Digitalisierungs-, Optimierungs-und Automatisierungsprojekte.

MKT-SB-v004-20240701-Öffentlich

TRIOVEGA GmbH
Kaninchenborn 31
23560 Lübeck, Deutschland
T: +49 451 39771 0
E: info@triovega.com

www.triovega.de