Stefan Gallenberger, Syskron GmbH

Cyberangriffe, Ausfälle, Innentäter – Anomalieerkennung in Industrie & kritischen Infrastrukturen

SYSKRON

Erstellt von: Max Mustermann
Datum: xx.xx.2021

Wer spricht?

Stefan Gallenberger

Cyber Security Consultant
Syskron Security

Phone: +49 9431 79857-1050
Mobil: +49 171 1846356

E-Mail: stefan.gallenberger@syskron.com

SYSKRON

Agenda

1. Bedrohungslage für produzierende Unternehmen der Getränkeindustrie
2. Wie kann man sich schützen?
   - Basisschutz einer Produktionsanlage
   - Bausteine für die eigene Fertigung auswählen
   - „Schubladen“ zur Sortierung der Bausteine, z.B. NIST Cyber Security Framework
3. Fragen

SYSKRON
Ihr Partner für Digitalisierung in der Getränke- und Liquid-Food-Industrie

SYSKRON

Für wen wir arbeiten – ganz konkret

Für Unternehmen aus diesen Branchen:


Nicht-alkoholische Getränke




Molkerei Produkte




Liquid Food

Alkoholische Getränke

Chemie, Pharmazie

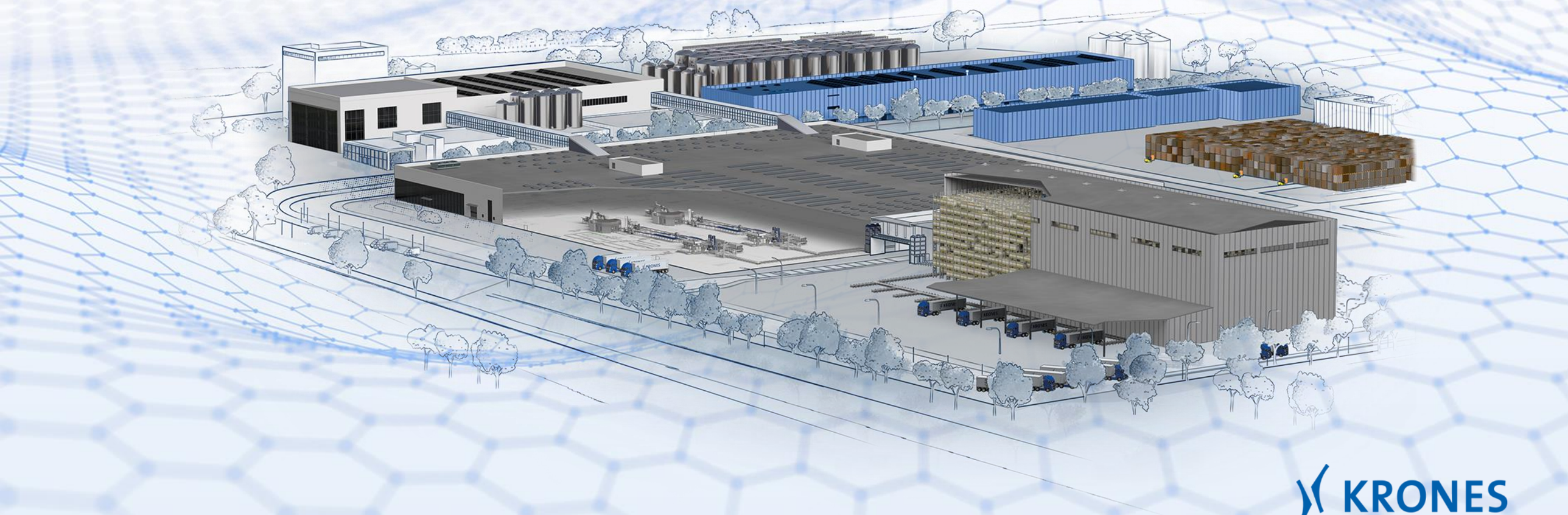


Kunststoff-Recycling

Home and Personal Care

Was wir tun – in einem Satz

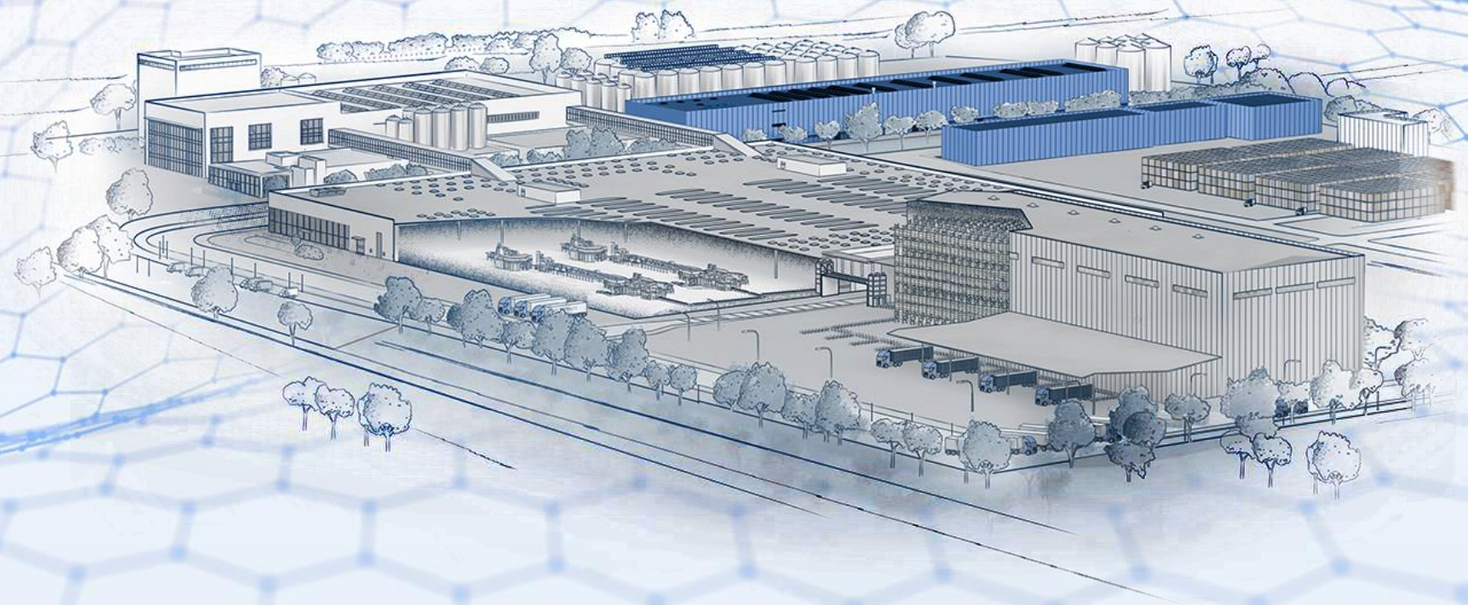
Wir versorgen unsere Kunden mit allem, was sie für ihre Wertschöpfung brauchen.



Was wir tun – ganz konkret

Wir entwickeln, planen und realisieren :

- Schlüsselfertige Fabriken
- Prozessanlagen für die Getränkeproduktion
- Abfüll- und Verpackungslinien
- Materialfluss- und Lagersysteme
- Recycling-Anlagen
  für PET und Polyolefine



Gibt es relevante Angriffe auf Produktionsanlagen in der Getränkeindustrie?

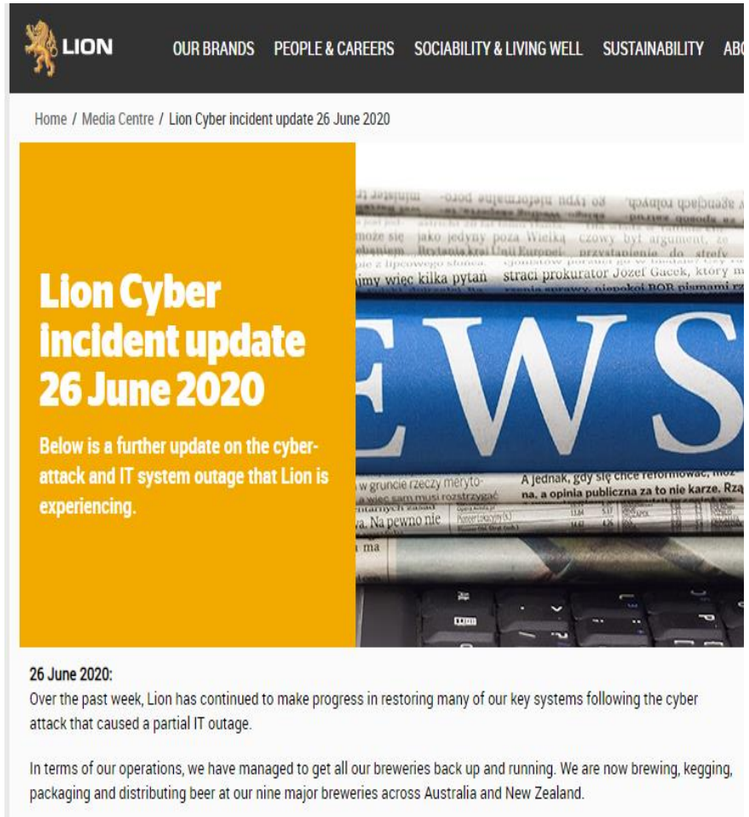
- Was ist die Motivation der Angreifer für zielgerichtete Angriffe auf Produktionsanlagen?
  → Lösegeld erpressen

- Was ist die Schadenshöhe bei Produktionsausfall einer Abfüll- und Verpackungsanlage für Getränke, bei angenommenen 24h Produktionsausfall?
  - Eine einzelne Produktionsline: 50.000 Behälter/h → bis zu 1,2 Mio Behälter/Tag

- Ein Angreifer kann problemlos eine mittlere sechsstellige Summe als Lösegeld fordern. Damit kann ein Angreifer auch mehrere Wochen pro Angriffsziel „investieren“

SYSKRON

Drei aktuelle Beispiele für erfolgreiche Angriffe



https://www.lionco.com/media-centre/lion-update-re-cyber-issue

https://www.zdnet.com/article/italian-beverage-vendor-campari-knocked-offline-after-ransomware-attack/

https://www.camparigroup.com/sites/default/files/downloads/20201204_Campari%20Group%20Press%20release.pdf

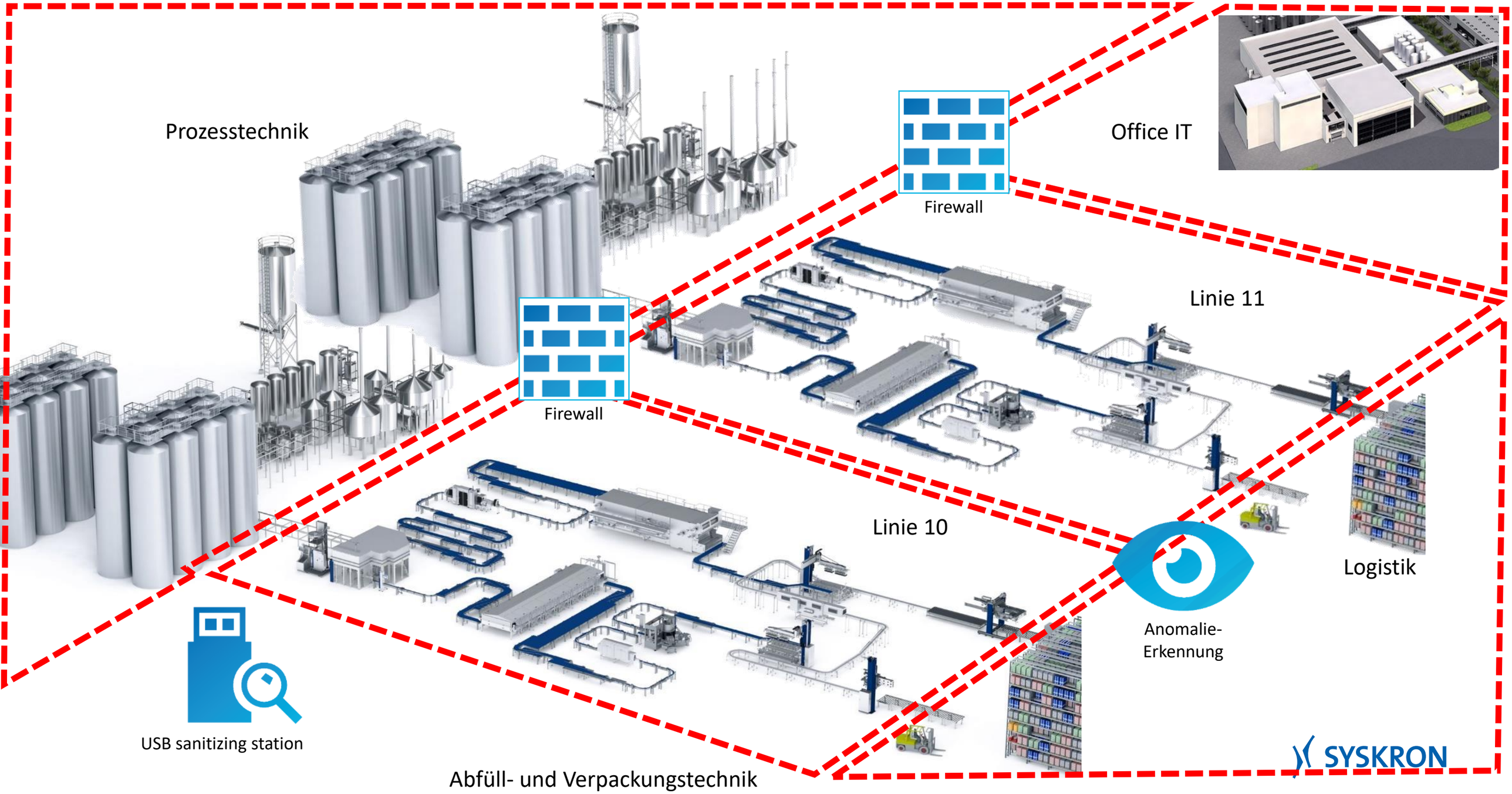
https://fm.cnbc.com/applications/cnbc.com/resources/img/editorial/2019/10/31/106216323-1572539411299gettyimages-953885094.1910x1000.jpeg

https://www.forbes.com/sites/leemathews/2021/03/14/cyberattack-disrupts-operations-at-molson-coors/

SYSKRON

Gerne pragmatisch starten, aber mit System, z.B. NIST Framework

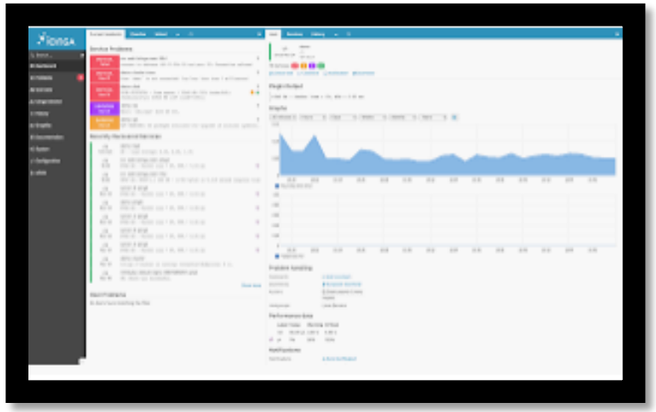
SYSKRON


Prozesstechnik
Office IT
Firewall
Firewall
Linie 11
Linie 10
Logistik
Anomalie-
Erkennung
USB sanitizing station
Abfüll- und Verpackungstechnik
SYSKRON

Respond: Security Operations Center - SOC

- Alarme aus den automatischen Systemen behandeln
- Alarme von Mitarbeitern behandeln
- Maßnahmen zur Eindämmung und Behebung eines Vorfalls einleiten
- Krisenstab einberufen (hoffentlich nur im Übungsfall)
- Häufig kommen aus dem SOC auch wichtige Hinweise zum Betrieb (z.B. Netzwerkprobleme)

Wichtig: Sicherheit ist eine tägliche Betriebsaufgabe!



SYSKRON

Ein tragfähiges Sicherheitskonzept besteht immer aus einer individuellen Zusammenstellung von mehreren Bausteinen

Identify

Cyber Security Maturity Assessment (CSMA)

Netzwerkanalyse einer Produktionslinie

Protect

Netzwerk-segmentierung (NG-Firewall)

Security Awareness Kampagne und Training

Information Security Management System (ISMS)

Detect

Anomalieerkennung

Schwachstellen-scan & Penetrationstest

Respond

Security Operations Center (SOC)

Notfallmanagement & Business Continuity Prozesse

Recover

Backup-Konzept

SYSKRON

Bei aller Planung die Umsetzung nicht vergessen!

SYSKRON

Zur Diskussion

- Produktionsanlagen sind häufig schwach geschützt und damit leichte Beute
- Sinnvolle „Zonierung“ des Produktionsnetzes durch Firewalls ist eine Minimalanforderung
- IT Sicherheit ist eine Aufgabe des TÄGLICHEN Betriebs der Produktionsanlagen
- Anomalieerkennung ist ein enorm wirkungsvoller Baustein, aber die Alarme müssen auch täglich von geeignetem Personal geprüft werden (Security Operation).
- Nicht auf eine Einzelmaßnahme fokussieren, es ist immer ein Bündel an Maßnahmen notwendig.
- Neben der der Technik auch an menschliche Schwachstellen denken (Phishing → Awareness), auch organisatorische Maßnahmen können gut wirken (USB-Richtlinie, Passwortrichtlinie)
- Gerne pragmatisch starten, aber systematisch, es gibt viele Systeme die helfen können (z.B. NIST CSF: Identify, Protect, Detect, Respond, Recover)
- Falls noch nicht geschehen: Bei „Identify“ starten, und den Status Quo feststellen.

Nun sind Sie dran…

Stefan Gallenberger

Cyber Security Consultant

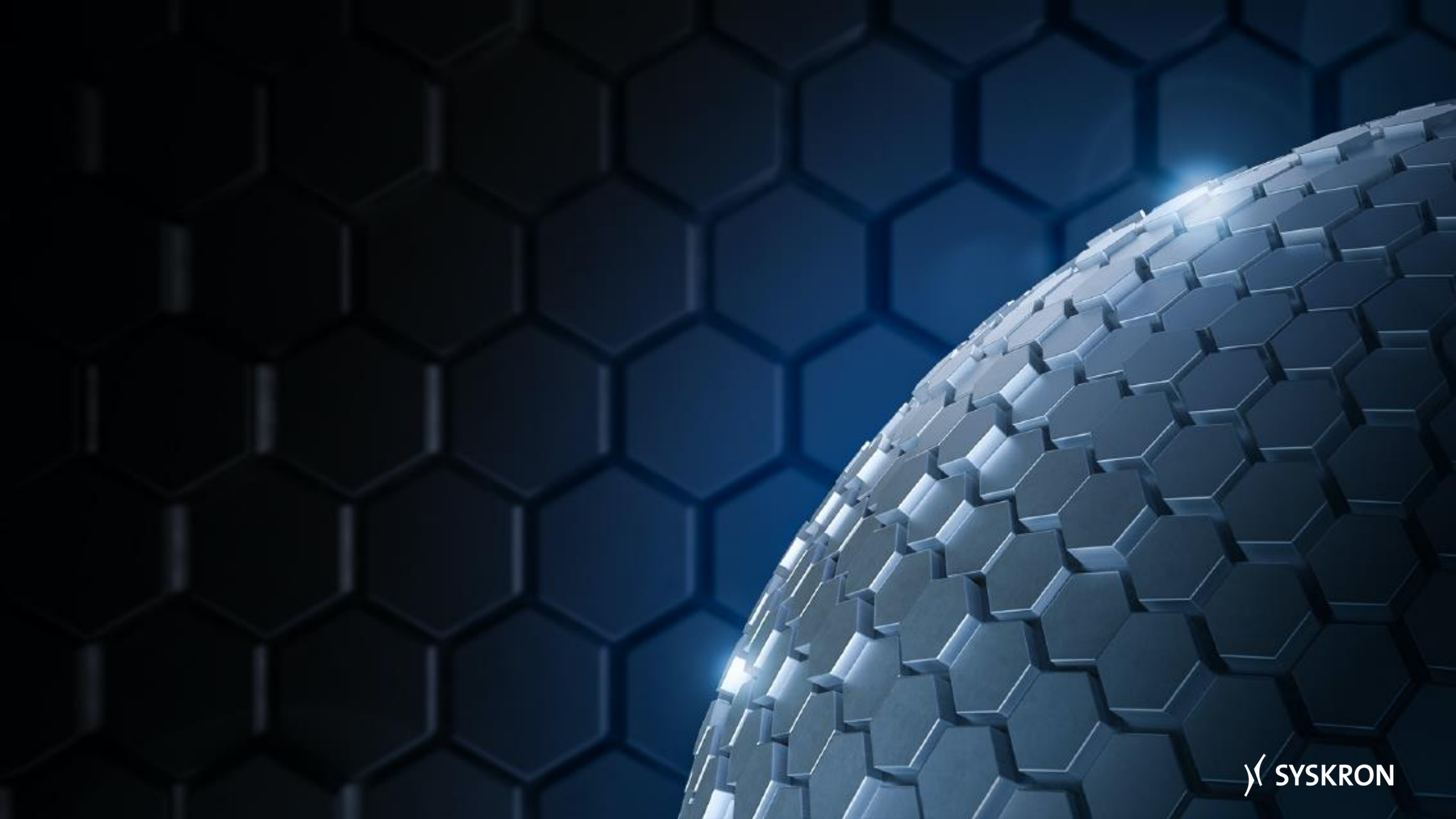
Syskron Security

Phone: +49 9431 79857-1050

Mobil: +49 171 1846356

E-Mail: stefan.gallenberger@syskron.com

SYSKRON


SYSKRON