22.03.2023: Executive Salon: IT – OT – Security.
Kernthesen der Diskussion

Smart-X: Autos, Maschinen, ganze Fabriken: Alles wird zunehmend zum software-gesteuerten Device. Das bringt nicht nur neue Sicherheitsanforderungen, sondern auch Update- und Supportbedarf: Unser Smartphone sortieren wir nach zwei Jahren veraltet aus. Das sollte bei Autos oder Maschinen nicht nötig werden. Und, eine zu hohem Grad zentralisierte Produktreihe birgt das Risiko eines größeren potentiellen Schadens, der durch einen Hackerangriff ausgelöst werden kann.

Nachholbedarf: Die IT hat Jahrzehnte Vorsprung bei der strukturierten Entwicklung einer Sicherheitsinfrastruktur – die Möglichkeiten von OT kommen mit großer Geschwindigkeit, hier entsteht viel Wildwuchs.

Einfach machen: Man kann die die Digitalisierung von Fabriken bis ins jede Detail planen – auf der grünen Wiese. Im Bestand fängt man einfach an. Ein Schritt nach dem anderen.

Ownership: Silos einreißen, agil arbeiten und klare Ownership: So wird aus einer ungesteuerten Konvergenz von IT und OT ein zielführender Prozess.

Stangenware? Software-as-Service ist für unzählige Anwendungen sinnvoll. Doch muss der Prozess auf die Software passen oder umgekehrt? Erfahrungsgemäß sollte die Software in Ruhe gelassen werden und Sonderlocken im Prozess angepasst werden.
Beispiel Gausche Verteilung oder 80/20-REgel: Für alle Prozesse, die von der Häufigkeit her unter die Glocke oder in die 80% fallen, sollte die Software implementierbar sein – die Ausreißer an den Seiten können vorerst vernachlässigt und später softwareseitig abgebildet werden.

Infomation & Strategy First Bevor man sich für eine Software und die Implementierung entscheidet, sollte die Bedarfssituation sowie die unterschiedlichen Szenarien gut verstanden werden. Dafür helfen Workshops, Simulationen und PoCs des Anbieters. Wenn der Anbieter selbst keine überzeugenden UseCases liefern kann, holt euch selbst Infos von Testimonials / anderen Kunden.

Resilience not Resistance: Schätze deine Cybersecurity richtig ein. Du kannst nicht alles verhindern. Aber du musst im Fall der Fälle handlungsfähig sein.

Technologie oder Mindset? Cybersecurity ist kein notwendiges Tool sondern muss als Mindset in einem Unternehmen verstanden werden, damit die zum Geschäft passenden Entscheidungen getroffen werden können.

Data is Key: OT muss viele Daten liefern, um die Transformation zur OT Tech-Company zu schaffen.

IT over OT(?!) IT wird schlussendlich die Hoheit übernehmen, auch wenn beide Bereiche sich kontinuierlich einander annähern müssen

Chance und Risko: Man kann riesige Sicherheitsmauern aufbauen. Und damit jeden Anwendungsfall erdrücken. Die Mauer sollte der Größe des Risikos angemessen sein.

Konstruktives Nein: Die sicherste Form der Digitalisierung ist die ausbleibende. Und jede Innovation bleibt auf der Strecke. Die Aufgabe der Cybersecurity ist nicht zu verbieten. Sondern zu begleiten und Business-Opportunitäten bestmöglich zu begleiten.