Unsere Spezial Workshops „Produzierendes Gewerbe“

Für Sie zur Auswahl: Drei Praxiskonzepte unserer zertifizierten Experten.

Basis-Paket	Business-Paket	Optimal-Paket
✓ Security Workshop mit Analyse der IT- und OT-Infrastruktur	✓ Basis-Paket zuzüglich	✓ Business-Paket zuzüglich
✓ Feststellung des IT-Security IST-Zustands	+ ISO 27001 Gap-Analyse	+ Security Roadmap zu den anstehenden Maßnahmen inklusive geschätzter Aufwände und Budgetierung
✓ Ergebnisdokument mit Handlungsempfehlungen	+ Schwachstellenscan für biszu 16 externe IP-Adressen	+ Fachlich versierter Support mit Blick auf die relevanten Aspekte der Cyber-Assekuranz
	+ Managementpräsentation der Ergebnisse aus Gap-Analyse, Schwachstellenscan und Security Workshop	

Was für Ziele haben Sie?
Wo dürfen wir Sie unterstützen?

Jetzt unverbindlich informieren!
Vereinbaren Sie Ihren kostenlosen Erst-Beratungstermin!

Tobias Kling
Teamleitung Vertriebsaußendienst

Tel. +49 711 88770-224
tobias.kling@to.com

Wissenswertes zur Thinking Objects GmbH

Die inhabergeführte Thinking Objects GmbH mit Sitz in Korntal bei Stuttgart ist seit 1994 als kompetenter IT-Dienstleister und Systemintegrator mit den Schwerpunkten IT-Sicherheit, IT-Infrastruktur, Internet-Technologie sowie Betrieb und Support in Rechenzentren tätig.

Seit über 25 Jahren bietet Thinking Objects marktgerechte Lösungen zur Unterstüzung, Entlastung, Optimierung und Sicherung des IT-Betriebs in großen und mittelständischen Unternehmen sowie Konzernen.

Erstklassige Referenzen bestätigen den Nutzen und die Qualität der Lösungen, zu den Kunden zählen z.B. Airbus DS Optronics, Lewa Pumpen & Systeme, MBtech Group, Schaefer Elektrotechnik.

Thinking Objects

Thinking Objects GmbH
Lilienthalstraße 2/1
70825 Korntal-Münchingen

+49 711 88770400
info@to.com
www.to.com

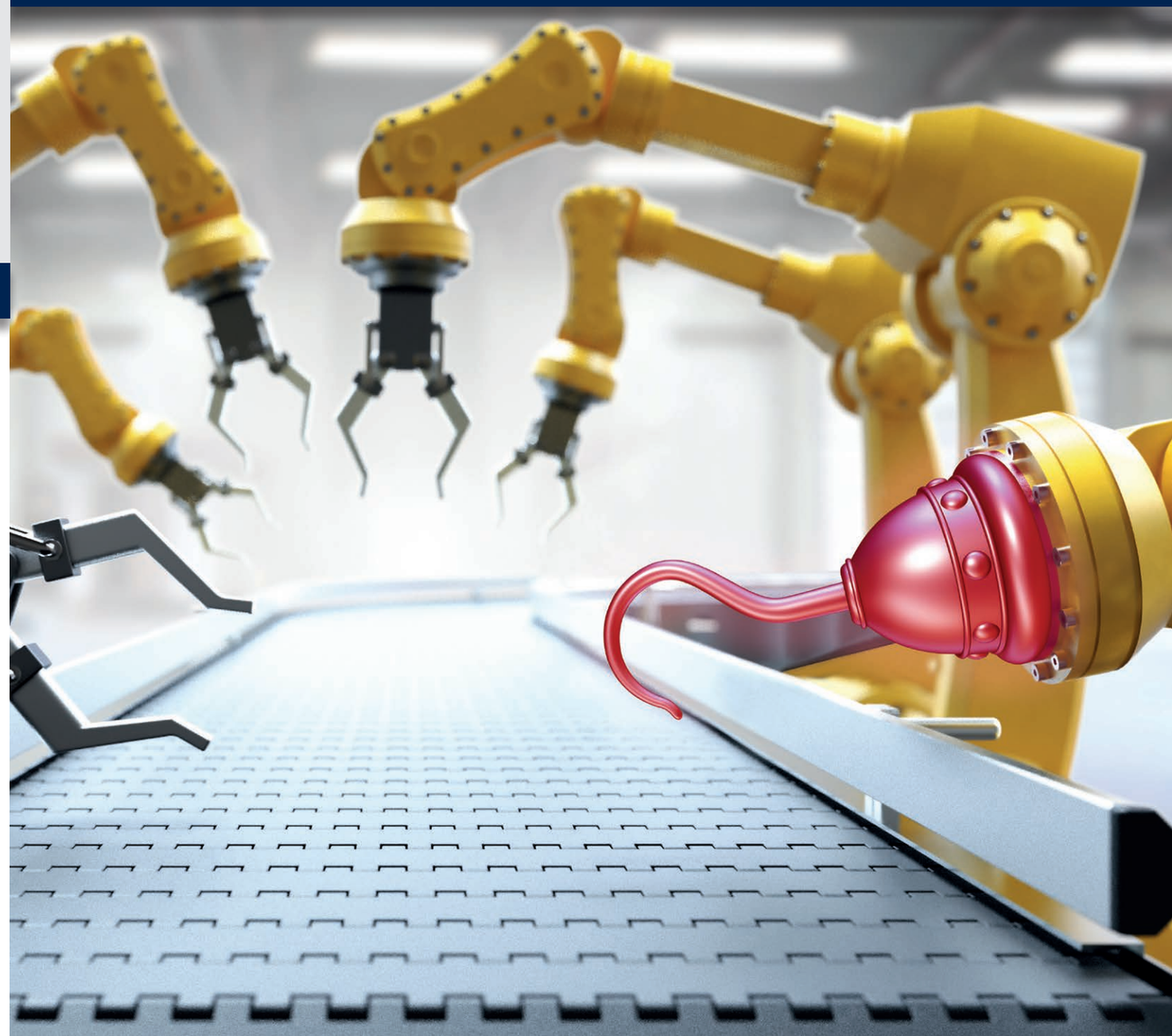
Management Summary

IT-Sicherheit im produzierenden Gewerbe.

Thinking Objects

Alptraum IT-Piraten: Wenn die Produktion still steht…

Warum Sie jetzt Ihre IT & OT auf den Prüfstand bringen müssen!



Cyberkriminalität bedroht Ihre industrielle Fertigung: Wie Sie wirksam für mehr Sicherheit sorgen!

Die Digitalisierung ist längst auch in der Fertigungsindustrie angekommen. Industrielle Automatisierungssysteme sind in allen Werkhallen vorhanden. Was zukunftsrelevant ist, birgt aber leider auch ein besonderes Risiko: **Die Produktion wird zum Angriffsziel für Cyber-Attacken.**

Wussten Sie, dass täglich weltweit mehr als 6 Millionen Cyberangriffe stattfinden? Immer häufiger gelten die Angriffe auch Industrieunternehmen. Den Firmen entstehen durch **Datendiebstahl, Datenmanipulation** oder durch **direkte Eingriffe in die Produktionsabläufe** schwere, ja sogar **existenzielle Schäden**.

Fatales Wiegen in Sicherheit

Trotz wachsender Bedrohungslage wird IT-Sicherheit in der Fertigung immer noch unterschätzt. Der vermeintlich schützende "air gap" löst sich durch die zunehmende Vernetzung der Produktionsanlagen immer weiter auf, Angriffsflächen für Cyberkriminelle vergrößern sich.

Angriffe auf die kritische Infrastruktur des verarbeitenden Gewerbes führen zu erheblichen finanziellen Verlusten. Wenn die Bänder für Tage, Wochen oder sogar Monate durch Ransomware stillstehen, entstehen einer aktuellen Studie von Sophos zufolge bei **deutschen Unternehmen im Durchschnitt 970.000 Euro Folgekosten**.

Die Bedrohungslage bleibt angespannt. In einer Befragung gab fast die Hälfte der Unternehmensvertreter aus deutschen KMUs an, dass sie von Cyberangriffen getroffen wurden. **Sich in Sicherheit zu wiegen wäre grob fahrlässig.** Erschwerend kommt hinzu, dass Angriffe immer raffinierter werden und häufig zu Spitzenzeiten stattfinden, wenn der Schaden am größten und der Druck auf die Geschäftsleitung am stärksten ist.

61% der Produktionsunternehmen hatten mit Cyber-Attacken zu kämpfen.[1]

Mehr als **1/3** der VDMA-Mitglieder berichten über Produktionsausfälle.[2]

Nachholbedarf: Vernetzte Produktion besonders gefährdet durch Cyber-Angriffe.[3]

Ransomware-Wiederherstellung kostet ø 970.000 Euro – das Doppelte i. Vgl. zu 2020.[6]

43% der Produktionsunternehmen hatten Ausfälle, die länger als 4 Tage andauerten.[1]

Cyber-Vorfälle gelten global als höchstes Geschäftsrisiko.[4]

82% rechnen mit weiterer Zunahme von Cyber-Attacken auf ihr Unternehmen.[5]

Nur **8%** der Unternehmen erhalten nach Lösegeldzahlung Daten vollständig zurück.[6]

(1) Trend Micro / Vanson Bourne Umfrage (2) VDMA-Umfrage CC Industrial Security (3) Fraunhofer IPT Whitepaper (4) Allianz Risk Barometer 2020 (5) Bitkom Studie Wirtschaftsschutz (6) Sophos State of Ransomware 2021

Ihr individueller Schutz

Die Herausforderungen und Bedrohungen für die vernetzte Industrie nehmen zu. Damit steigt die Verantwortung für die IT und die OT der Produktion.

Nehmen Sie jetzt eine Kursbestimmung für Ihre Firma vor:

- Welche Schutzmechanismen sind im industriellen Sektor erforderlich?
- Wie lassen sich Produktionsabläufe in Ihrer Firma vor Angriffen schützen?
- Wie unterscheidet sich Sicherheit in der IT von Sicherheit in der OT – und wo liegen die Synergien?
- Welches sind die wirksamen Maßnahmen im Falle einer Attacke?
- Wie lassen sich menschliche Fehler und menschliche Unachtsamkeit vermeiden?

Ihren **Wunschzettel an die Zukunft** kennen wir (noch) nicht. Aber wir sind dafür da, dass **die dafür notwendige IT-Security** auch gewährleistet ist.

Was bedeutet IT-Security bei geplanten Vorhaben, wie z.B.:

Industrie 4.0, Industrial Internet of Things (IIoT) und Künstliche Intelligenz (KI): Digitalisierung im Produktionsprozess und Einsatz von (teil-) autonomen Maschinen.

Smart Factory: Flexibilisierung und hochgradige Anpassung der Produktion für Kleinserien und Individualisierung - vom Produktlebenszyklus hin zum Servicelebenszyklus.

Augmented Reality zur Visualisierung von Maschinendaten und Kombination mit Analysedaten in Echtzeit: Modernisierung von Wartungsdienstleistungen (Remote Access, Fernwartung) sowie VR- und Mixed Reality-basierte Schulungen.

Die 7 großen Bedrohungen. Ihr Schutz vor den IT-Piraten.

Nehmen Sie jetzt eine Standortbestimmung in Ihrem Unternehmen vor, machen Sie eine Risikoanalyse der Cyber-Bedrohungslage!

Aus der jahrzehntelangen Erfahrung wissen die Experten von Thinking Objects wo auch in gut geführten Firmen noch Optimierungspotenziale in der IT-Security möglich sind. Nutzen Sie dieses Fachwissen, um sich proaktiv gegen Angriffe verteidigen zu können.

Machen Sie sich bewusst, dass alle Systeme Ihres Unternehmens verwundbar sind. Zu den großen Bedrohungen zählen unter anderem diese 7 Themenfelder. Wir liefern Ihnen dazu auch gleich einige Denkanstöße.

1 „Wechseldatenträger"

Eigentlich ein banaler Vorgang, aber blitzschnell hat man ein ernsthaftes Problem. Denn Schadsoftware lässt sich kaum einfacher einschleppen und übertragen als mit „Wechseldatenträgern". Sei es durch USB-Sticks oder auch über den USB-Port an Werkzeugmaschinen angeschlossene Smartphones.

Wie ist der Umgang mit Wechseldatenträgern bei Ihnen verbindlich geregelt? Haben Sie „Schleusen" mit permanent aktualisierten Virenschutzscannern?

2 Zugangsberechtigungen und Passwörter

Ein „uraltes Thema" – aber noch immer ist der Zugang zu Geräten, zur IT-Infrastruktur in vielen Fällen nicht wirksam gesichert. Das betrifft nicht nur Bereiche innerhalb der Firma. Viele Mitarbeitenden haben, auch durch Home-Office und „bring your own device", Zugriff von unterwegs auf Ihr System. Das birgt jede Menge Gefahren.

Wie wirksam sind Ihre Zugriffs- und Berechtigungssysteme? Gibt es eine funktionelle Authentifizierung und Autorisierung? Wie sind Firmensmartphones, Laptops etc. sinnvoll verschlüsselt?

3 Risiken von Netzanschlüssen

Neue, vernetzte Fertigungsprozesse führen zu einer vermehrten Integration von Produktionsmaschinen in das Firmen-LAN. Auch die Anforderungen durch Production Planning Systems, PPS oder die Kommunikation mit Warenwirtschaftssystemen machen eine klare IT-/OT-Securitystrategie nötig.

Wie haben Sie Ihre Firewalls, Ihre Monitoring-Lösungen etc. strukturiert? Wie steht es um die Aktualität der Programme?

4 Risikofaktor „Internet"

Immer mehr Services sind durch das Internet Teil des Alltags geworden. Sei es die Anbindung an die Kunden-IT für die Auftragsabwicklung oder für Remote-Services.

Setzen Sie bereits auf Zertifikate für externe Zugänge? Wie gut sind Ihre 2-Faktoren-Authentifizierungen? Haben Sie sich schon mit einem „Quarantäne-Netzwerk" beschäftigt, in das nicht regelkonforme Zugriffe automatisiert verschoben werden?

5 NC-Programme und Daten

Unzureichende Zugriffs- und Berechtigungssysteme machen den Datendiebstahl und Datenverlust leicht. Schadsoftware mittels Phising ist blitzschnell eingeführt.

Haben Sie Ihre Netze segmentiert? Wie steht es um die Einrichtung von VPNs, die Deaktivierung von Internet-Zugängen?

6 Die Menschen in Ihrem Unternehmen

Die klassische IT und die OT müssen miteinander verknüpft werden. Denn egal ob es um IoT oder Industrie 4.0 geht, der Innovationsdruck bringt Gefahren mit sich. Ein infizierter Laptop, eine Phisingmail kann genügen um die gesamte Produktion für Wochen lahm zu legen.

Nutzen Sie Pentests, um sowohl Klarheit über die Gefahren zu haben, wie auch die Belegschaft zu sensibilisieren? Gibt es klare Regeln „wer darf was?"

7 Bedenken in puncto Budget

Über die großen Investition in Maschinen und Anlagen wird lange und intensiv diskutiert. Die vergleichsweise minimalen Aufwendungen für die Sicherheit von IT und OT werden gerne ausgeblendet. Außerdem unterliegt man gerne mal dem Trugschluss, dass man ja „Virenschutzprogramme" und eine Firewall hat. Wenn's nur so einfach wäre. Profitieren Sie vom fairen Preis-/Leistungsverhältnis bei Thinking Objects.

Nutzen Sie die herstellerneutrale Fachberatung der IT-Security Spezialisten von Thinking Objects.