Fraunhofer IAO

Dr. Christian Schunck, Cybersecurity Region Stuttgart Meetup bei Fraunhofer IAO März 2026

»OT-Security im industriellen Mittelstand«

Was ist OT? Betriebstechnik aus Hard- und Software, die für die Steuerung von Anlagen und Prozessen eingesetzt wird.

Motivation für OT-Security

Lila Cyber-Pause: Hacker legen Milka-Schokoladenfabriken lahm

In der Papierfabrik Perlen stehen die Maschinen still – wird das Zeitungspapier knapp?

Wegen eines Cyberangriffs auf ihr IT-System musste die einzige Zeitungspapierfabrik der Schweiz am Freitag die Produktion einstellen. Frühestens Anfang nächster Woche könne sie wieder in Betrieb genommen werden, heisst es. Es ist mit Lieferengpässen zu rechnen.

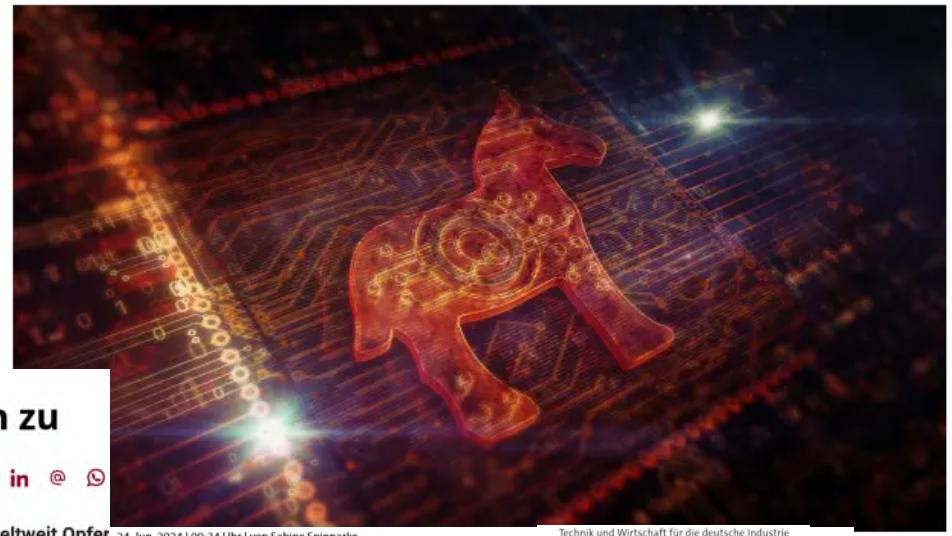
Giorgio V. Müller
07.01.2022, 17.39 Uhr

Hören Merken Drucken Teilen

Akira-Ransomware schlüpft über Webcam an IT-Schutzlösung vorbei

Eigentlich ist das Firmennetz über eine Schutzsoftware geschützt, die auch anschlägt. Trotzdem konnte ein Trojaner über einen Umweg PCs infizieren.

26



CYBERANGRIFF IN NORWEGEN

Hacker reißen Ventile eines Staudamms auf

Durch den Angriff gab es an einem Staudamm in Norwegen für vier Stunden einen Wasserabfluss um 497 Liter pro Sekunde über Plan.

in Pocket speichern merken

2. Juli 2025, 13:00 Uhr, Marc Stöckel

(Bild: pixabay.com / daramsri)

Fortinet Report zeigt dramatische Entwicklungen auf

Cyberangriffe auf OT-Systeme nehmen zu

26.09.2024 Lesezeit: ca. 3 Minuten

Laut der aktuellen Fortinet Studie wurde 2023 fast jedes zweite Unternehmen weltweit Opfer eines OT-Angriffs. Besonders besorgniserregend ist der starke Anstieg der Vorfälle im ersten Halbjahr 2024: Bereits 73 Prozent der Unternehmen waren betroffen. Mit der zunehmenden Komplexität und Häufigkeit gezielter OT-Angriffe stehen viele Unternehmen vor der Herausforderung, ihre Sicherheitsstrategien anzupassen. Können die Erkennungsmethoden mit der rasanten Entwicklung der Bedrohungen mithalten? Die Studie liefert wichtige Erkenntnisse und Handlungsempfehlungen.

24. Jun. 2024 | 09:34 Uhr | von Sabine Spinnarke

Technik und Wirtschaft für die deutsche Industrie

Produktion

Ransomware-Angriffe

Cybersecurity: Der Wurm im OT-Netz

Black Basta kostete die Industrie über 100 Millionen Euro an Lösegeld. Erst Anfang 2024 konnte die Ransomware entschlüsselt werden. Zwar attackiert Ransomware keine Produktionsanlagen, dennoch verursacht sie Stillstände.

Fraunhofer IAO

Möglicher Ablauf eines OT-Sicherheitsvorfalls

Die Malware läuft auf zwei Füßen in die Fabrik

ABLAUF

01

Routinewartung durch einen externen Dienstleister
Ein externer Servicetechniker besucht das Unternehmen für planmäßige Wartungsarbeiten an einer CNC-Fräsmaschine. Der Techniker verbindet seinen Laptop mit der Maschinensteuerung, um Diagnosen durchzuführen und Software-Updates einzuspielen.

02

Unbemerktes Einschleusen von Malware
Der Laptop des Technikers ist unbemerkt mit Malware infiziert. Diese Schadsoftware wurde zuvor durch einen Phishing-Angriff auf den Dienstleister eingeschleust. Beim Anschluss an die Maschinensteuerung überträgt sich die Malware auf das interne OT-Netzwerk des Unternehmens.

03

Ausbreitung im OT-Netzwerk
Aufgrund fehlender Netzwerksegmentierung und mangelnder Sicherheitsmaßnahmen kann sich die Malware ungehindert im gesamten Produktionsnetzwerk ausbreiten. Steuerungsparameter werden manipuliert, und es kommt zu ungewöhnlichen Maschinenbewegungen.

04

Produktionsausfall und Schäden
Innerhalb weniger Stunden führen die Manipulationen zu Fehlfunktionen mehrerer Produktionsanlagen. Maschinen stoppen abrupt oder produzieren fehlerhafte Teile. Um größere Schäden zu vermeiden, entscheidet das Management, die gesamte Produktion vorübergehend einzustellen.

05

Reaktion und Schadensbegrenzung
Das Unternehmen ruft ein Krisenteam zusammen und konsultiert externe OT-Security-Experten. Die Spezialisten identifizieren die Malware und beginnen mit der Analyse und Bereinigung der Systeme. Die Ursachenforschung ergibt, dass die Sicherheitslücke durch den infizierten Laptop des Servicetechnikers entstanden ist.

FOLGEN

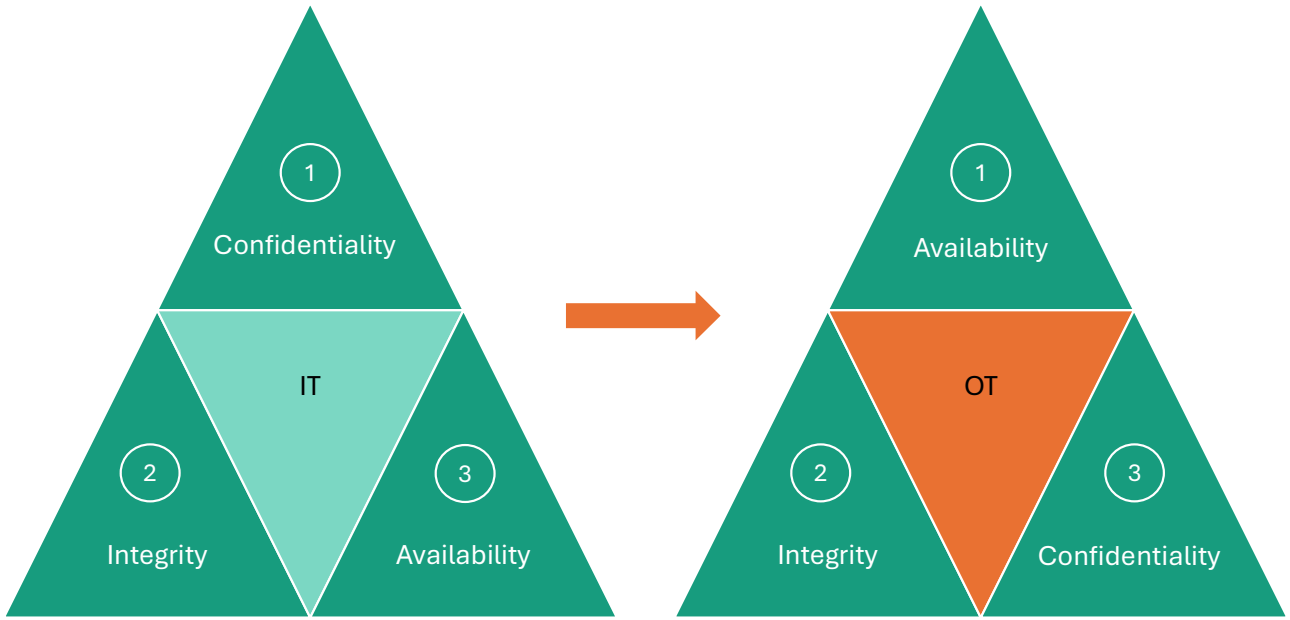
Finanzielle Verluste
Der Produktionsstillstand über mehrere Tage verursacht erhebliche Umsatzeinbußen. Zusätzlich entstehen Kosten für die Schadensbehebung und externe Beratung. Insgesamt beläuft sich der finanzielle Schaden auf mehrere hunderttausend Euro.

Reputationsschaden
Lieferverzögerungen führen zu Unzufriedenheit bei Kunden. Das Vertrauen in die Zuverlässigkeit und Professionalität des Unternehmens wird beeinträchtigt. Kundenbeziehungen sind gestört, Folgeaufträge gefährdet.

Herausforderung: OT ist anders als IT

Wird häufig übersehen

CIA-Dreieck: unterschiedliche Prioritäten zwischen IT und OT



	IT-Security	OT-Security
Lebenszyklus	Kurzfristig (in der Regel wenige Jahre)	Langfristig (oft mehrere Jahrzehnte)
Update-Management	Regelmäßige Updates und Patches	Seltene Updates; Risiko von Betriebsunterbrech-ungen beim Patchen
Technologien & Systeme	Standardisierte Hard- und Software	Spezialisierte & proprietäre Systeme und Protokolle
Auswirkung von Sicherheits-vorfällen	Datenverlust, finanzielle Schäden durch Datenlecks	Physische Schäden, Produktionsausfall, Gefahr für Mensch & Umwelt

Besondere Herausforderungen der OT

Integration von IT und OT

Die zunehmende Vernetzung von OT-Systemen mit IT-Netzwerken öffnet neue Angriffsvektoren.
Ein Sicherheitsvorfall in der IT kann jetzt die OT beeinflussen und umgekehrt.
Dies erfordert einen ganzheitlichen Sicherheitsansatz, der beide Bereiche berücksichtigt.

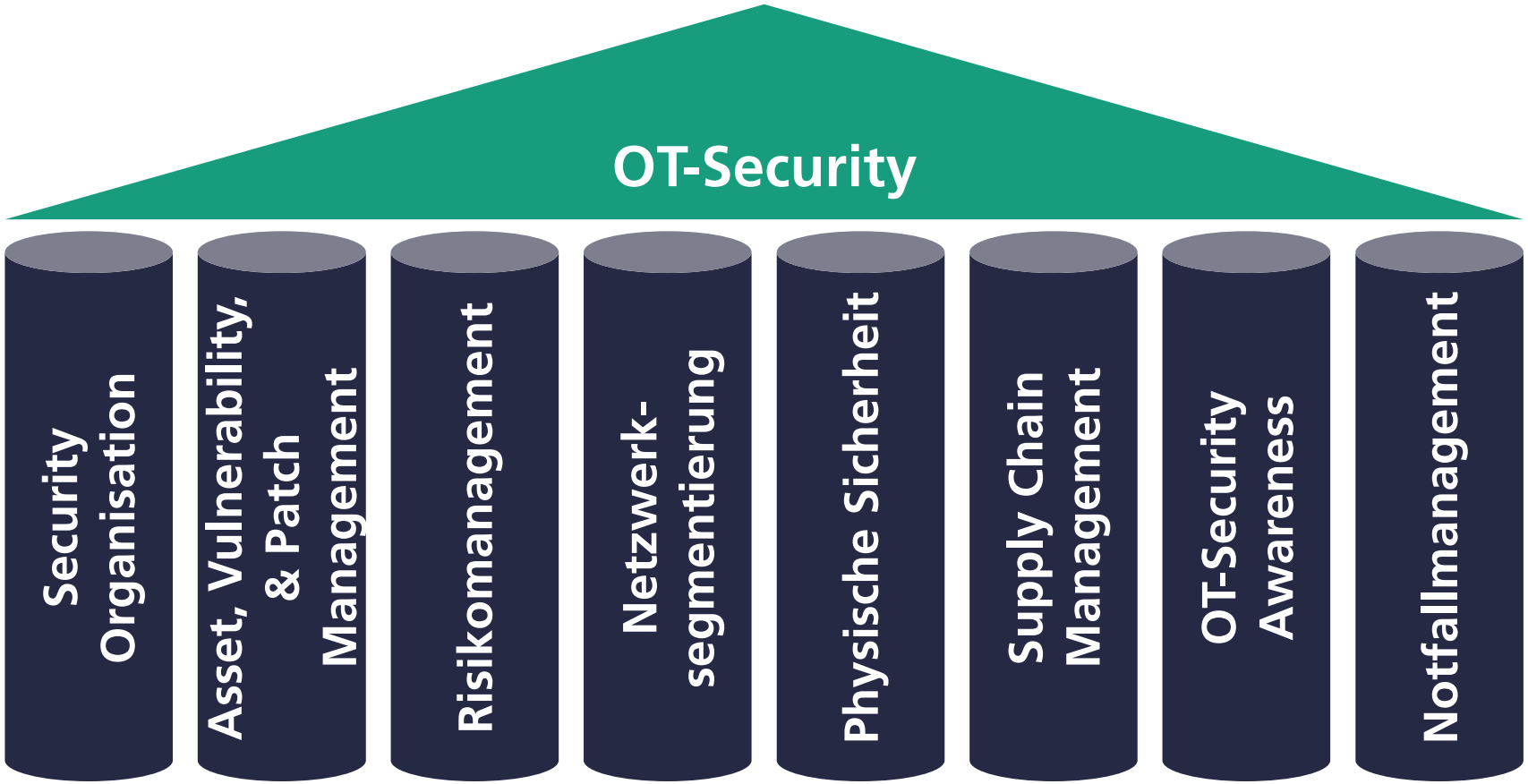
Fachkräftemangel und Wissenstransfer

OT-Security erfordert spezielle Kenntnisse, die sowohl IT- als auch OT-Expertise umfassen.
Der Mangel an Fachkräften mit diesem hybriden Wissen stellt Unternehmen vor Herausforderungen bei der Umsetzung effektiver Sicherheitsstrategien.

Regulatorische Anforderungen

In einigen Branchen, insbesondere in kritischen Infrastrukturen, gibt es strenge gesetzliche Vorgaben für die Sicherheit von OT-Systemen.
Unternehmen müssen Compliance sicherstellen, was zusätzliche Ressourcen bindet.

Besondere Herausforderungen der OT



ROADMAP

Erste Schritte zur grundlegenden OT-Security

Security Organisation

1. Benennung der OT-Sicherheitsverantwortlichen (z. B. OT-Security Officer)
2. Etablierung der OT-Security als Thema in IT- und OT-Meetings
3. Definition der Zusammenarbeit zwischen IT und OT

Assetmanagement

4. Identifizierung und eindeutige Erfassung der Kronjuwelen
5. Erfassung der wichtigsten Informationen der Assets für die Security

Notfallmanagement

6. Benennung des OT-Notfallteams und Definition der grundlegenden Verantwortlichkeiten
7. Dokumentation der ersten Melde- und Eskalationsketten für OT-spezifische Vorfälle
8. Erste Version der Notfall und Wiederherstellungs-dokumentation erstellen und sicher ablegen

Risikomanagement

9. Konzept für eine strukturierte Erfassung der Risiken
10. Erste Risikobewertung für „Kronjuwelen“ basierend auf Bedrohungen und möglichen Auswirkungen
11. Umsetzung erster grundlegender Sicherheitsmaßnahmen zur Risikominimierung

Organisation von IT/OT-Security

Leistungsspektrum definieren – Verantwortlichkeiten etablieren

Standardisierte Prozesse einführen

- IT und OT wachsen zusammen
- Organisatorische Basis muss geschaffen werden
- Grundlage sind klar definierte Prozesse und Verantwortlichkeiten
- Gewerke müssen einbezogen werden
- Ziele:
  - Abgesicherte Produktionsanlagen
  - Business Continuity
  - IT in der Produktion zukunftsfähig aufsetzen

Herausforderungen

- OT-Services definieren und Verantwortlichkeiten festlegen
- Darauf ein OT-Service Management aufbauen
- OT-Security und Prozesse über Gewerke hinweg standardisieren
- Regelmäßigen Wissensaustausch etablieren

Assetmanagement

Man kann nur schützen, was man kennt.

Nutzen von Assetmanagement

- Kontrolle und Übersicht über die eigenen Systeme und Sicherheitslandschaft.
- Priorisierung von Tätigkeiten anhand von Business-Kritikalität und der Sicherheits-Kritikalität von Assets
- Optimierung existierender Prozesse und Maßnahmen durch Erfassung des Ist-zustandes
- Automatisierung von Prozessen.
- Aktueller Wissenstand über Assets und ihren Zustand

Herausforderungen

- Es gibt keine Silver-Bullet-Lösung. Jede IT/OT-Landschaft ist anders.
- Starke Heterogenität, vor allem im OT-Bereich.
- OT-Geräte sind sehr anfällig für Veränderungen oder unerwartetes Verhalten im Netzwerk.
- „Einfach Neustarten und Patchen“ funktioniert „noch“ nicht im OT-Bereich
- Wie halte ich den Wissensstand aktuell?

Assetmanagement

Scannen, Scannen, Scannen!

Methoden für das Erfassen von Assets

- Aktives Scannen: Aktives Abfragen der Netzwerkumgebung. Welche Geräte sind in dem Netzwerk und was für Services laufen auf ihnen?
- Passives Scannen: Beobachten der Netzwerkumgebung. Welche Geräte und Services kommunizieren in der Umgebung und mit wem?
- Agentenbasiertes Scannen: Detaillierte Überwachung eines einzelnen Gerätes mit einem darauf installierten Agenten.
- Manuell: Manuelles Erfassen von Assetinformationen in Tools oder Listen.

Herausforderungen

- Aktives Scannen: Kann zu Komplikationen, unerwartetem Verhalten und Netzwerküberlastung führen.
- Passives Scannen: Finde nur Assets die auch wirklich kommunizieren.
- Agentenbasiertes Scannen: Benötigt einen Installierten Agenten. Nicht immer möglich.
- Manuell: Mühsam aber manchmal unumgänglich

Netzwerksegmentierung

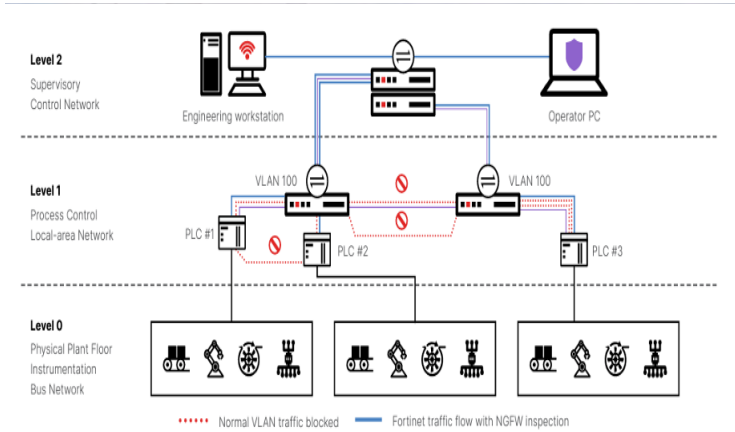
Kill-chains unterbrechen

Nutzen von Netzwerksegmentierung

- Minimierung von Risiken
- Schutz von besonders anfälligen Legacy-Systemen
- Isolierung im Falle der Kompromittierung
- Reduzierung der Angriffsfläche
  - Vermeiden unnötiger Kommunikation zwischen Geräten
  - Verringerung des Netzwerktraffics
- Verfügbarkeit der Produktion erhalten

Herausforderungen

- Segmentieren ist nicht Trennen.
- Segmentierung bedeutet immer erhöhte Aufwände: trade-offs
- Jede Umgebung und Produktionszelle kann andere Anforderungen haben: z.B. bzgl. Latency
- Isolierter Betrieb nicht immer möglich: manche Anlagen müssen miteinander kommunizieren.
- Wartung und sicherer Remote Access



https://www.fortinet.com/content/dam/fortinet/images/cyberglossary/vlan-traffic-blocked.png

Notfallmanagement

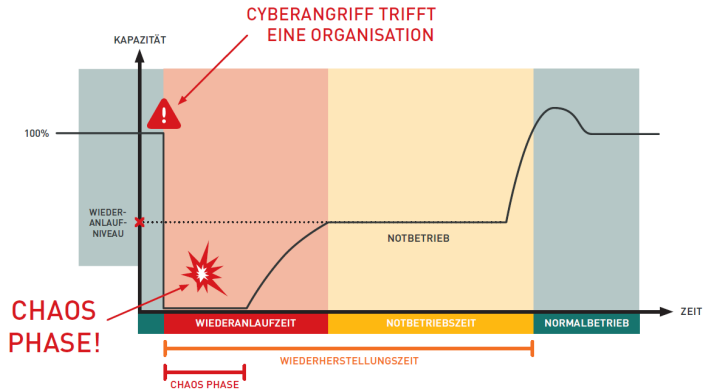
Kein Backup? Kein Mitleid.

Schäden minimieren

- Chaosphase bei einem Vorfall so kurz wie möglich halten
- Vorbereitete und geplante Maßnahmen schnell umsetzen.
- Klar definierte Ansprechpartner in IT/OT Security und den Gewerken sind erreichbar und kennen sich
- Redundante Kommunikationssysteme
- Eingespielte Entscheidungsgremien
- Einbeziehung von Dritten planen z.B. in Form von Allianzen

Herausforderungen

- OT-Notfallteam aufbauen - Expertise in den Gewerken mit SOC verknüpfen
- Meldeketten etablieren – Eskalationsstufen definieren – Einzelentscheidungen vermeiden
- Dokumentation und Entscheidungshilfen vorhalten – von technischen Plänen bis zu Fragenkatalogen zur Triage
- Backups vorhalten – Wiederherstellungszeiten kennen
- Üben, üben, üben, üben, …



Studie OT-Security im industriellen Mittelstand

https://www.i40-bw.de/studie-ot-security/

Studieninhalte

- **Grundlagen**
- **Handlungsfelder**
  - Herausforderungen
  - Maßnahmen
  - Prozesse und Prinzipien
  - …
- **Praxisnahe Lösungsansätze für den industriellen Mittelstand**

3

Inhalt

1. Management Summary
1.1 Zielsetzung der Studie
1.2 Wesentliche Erkenntnisse
1.3 Empfehlungen
2. Einführung
2.1 Hintergrund und Relevanz der OT-Security in der digitalen Transformation
2.2 Fokus auf den industriellen Mittelstand
2.3 Methodik: Literatur- und Marktrecherche, Experteninterviews und Fallstudien
2.4 Beispielhafte Fallstudie
3. Grundlegende Bedeutung von OT-Security im industriellen Mittelstand
3.1 Definition und Abgrenzung von OT-Security
3.2 Aktuelle Bedrohungslage und Risiken
3.3 Besondere Relevanz der OT-Security für den industriellen Mittelstand
3.4 Spezifische Herausforderungen und Chancen für den Mittelstand
4. Handlungsfelder der OT-Security
4.1 Security Organisation
4.2 Asset-, Vulnerability- und Patchmanagement
4.3 Risikomanagement
4.4 Netzwerksegmentierung
4.5 Physische Sicherheit
4.6 Supply Chain Management
4.7 OT-Security-Awareness
4.8 Notfallmanagement
5. Praxisnahe Lösungsansätze für den industriellen Mittelstand
5.1 Die absoluten Basics und erste weitergehende Schritte
5.2 Unterstützungsangebote
5.3 Weiterführende Materialien
6. Ausblick
7. Anhang
7.1 Glossar
7.2 Verfasser der Studie
8. Impressum

OT-SECURITY IM INDUSTRIELLEN MITTELSTAND

Handlungsfelder und Lösungen für die sichere digitale Transformation

ALLIANZ Industrie 4.0 BADEN-WÜRTTEMBERG

Fraunhofer IAO

Innovationsnetzwerk OT-Security

Ausfälle verhindern, Sicherheitslücken schließen

- **Das Innovationsnetzwerk richtet sich an**
  Produktionsleitung, Mitarbeitende in der IT- und OT-Sicherheit, IT- und OT-Organisation, Industrie 4.0-Verantwortliche, Betreiber kritischer Infrastrukturen (KRITIS)

- **Wo? Wann?**
  Neue Runde ab September 2026, 6 Netzwerktreffen

- **Vorteile**
  Lebendiges Netzwerk, Voneinander Lernen
  Gebündeltes Wissen aus Forschung und industrieller Beratung
  Vermeidung von Fehlern und unnötigen Kosten
  Neue Impulse für eigene Initiativen
  Verbesserte IT/OT Sicherheit

Mehr Infos und Anmeldung

Fraunhofer IAO

Lernlabor Cybersicherheit

Faktor Mensch

- Interaktion mit Demonstratoren, um verschiedene Formen von Cyberangriffen zu erleben
- Online-/Offline-Schulungen mit dem Fokus auf den menschlichen Faktor der Cybersicherheit
  - Finanz- und rechnungsbetrug verhindern
  - Empathisch Policy Engineering
  - Konfliktlösung bei Sicherheitsmaßnahmen
- **Wo?** Bildungscampus Hochschule Heilbronn, Gebäude 17, Raum S0.21
- **Wann zu besuchen?**
  Kontakt für Terminvereinbarungen

Mehr Infos→
https://www.iao.fraunhofer.de/lernlabor-cybersicherheit

Vielen Dank für Ihre Aufmerksamkeit

Dr. Christian Schunck

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

christian.schunck@iao.fraunhofer.de

+49 711 970 2430