infinigate
spark your growth

OT-Security

So schützen Sie relevante Infrastrukturen, Arbeitsumgebungen und Menschen

infinigate

OT-Security – Schützen Sie Ihre Automatisierung und Steuerungssysteme

OT-Security (Operational Technology Security) bezeichnet Maßnahmen und Technologien zum Schutz industrieller Kontrollsysteme (ICS), Prozesssteuerungssysteme und anderer kritischer Infrastrukturen vor Cyberbedrohungen.

Im Gegensatz zur IT-Security, die sich primär auf Netzwerke, Server und Daten konzentriert, liegt der Fokus der OT-Security auf der Absicherung physischer Geräte, Maschinen und Anlagen. Viele dieser Systeme wurden ursprünglich nicht für eine direkte Anbindung ans Internet (z. B. Fernwartung) entwickelt und basieren oft auf veralteten Betriebssystemen wie Windows XP oder Windows 7. Dadurch sind sie besonders anfällig für Cyberangriffe.

Typische Einsatzbereiche von OT-Security:

1 **Fertigungsindustrie**
OT-Systeme steuern und automatisieren Produktionsprozesse, überwachen Maschinen und sichern die Produktqualität.

2 **Energiesektor**
Hier wird OT zur Steuerung und Überwachung von Kraftwerken, Stromnetzen sowie weiteren Energieinfrastrukturen eingesetzt – von der Erzeugung über die Übertragung bis hin zur Verteilung.

3 **Wasser- und Abwasserwirtschaft**
OT-Systeme steuern Wasseraufbereitungsanlagen, Pumpstationen und Verteilungssysteme. So wird eine zuverlässige Wasser- und Abwasserversorgung gewährleistet.

4 **Transportwesen**
OT kommt in der Überwachung und Steuerung von Verkehrssignalanlagen, Bahn- und Straßenverkehrssystemen sowie Flughäfen zum Einsatz – für einen sicheren und effizienten Personen- und Gütertransport.

5 **Gesundheitswesen**
In Krankenhäusern und medizinischen Einrichtungen steuern MIoT-Systeme unter anderem medizinische Geräte und Patientenüberwachungssysteme. Sie tragen entscheidend zur Versorgungssicherheit und zum Schutz der Patienten bei.

Warum eine funktionierende OT-Infrastruktur unverzichtbar ist

Eine zuverlässige OT-Infrastruktur ist aus mehreren Gründen von zentraler Bedeutung:

1. **Vermeidung finanzieller Risiken**
Betriebsunterbrechungen und Produktionsstillstände können erhebliche finanzielle Schäden verursachen – etwa durch Umsatzverluste, hohe Instandsetzungskosten und Reputationsschäden für das Unternehmen.

2. **Schutz von Menschen und Umwelt**
Der Ausfall von OT-Systemen kann die physische Sicherheit von Mitarbeitenden, der Öffentlichkeit und der Umwelt gefährden – insbesondere in kritischen Infrastrukturen.

3. **Abwehr von Cyberbedrohungen**
Cyberangriffe auf OT-Systeme können nicht nur zu physischen Schäden führen, sondern auch zum Diebstahl sensibler Daten oder zur gezielten Sabotage von Abläufen. Solche Vorfälle beeinträchtigen langfristig die Betriebssicherheit und Wettbewerbsfähigkeit eines Unternehmens.

4. **Erfüllung gesetzlicher Anforderungen (NIS2, CRA, Maschinenverordnung)**
Mit Inkrafttreten der deutschen **NIS2-Richtlinie** ab 2026 und des **Cyber Resilience Act (CRA) und Maschinenverordnung** ab 2027 steigen die Anforderungen an die Cybersicherheit in Deutschland erheblich.Betroffen sind insbesondere Betreiber wesentlicher und wichtiger Einrichtungen, Anlagen- und Maschinenbauer sowie Dienstleister.

5. Die Gesetze schreiben umfassende **Risikomanagementmaßnahmen** vor – darunter Risikoanalysen, Sicherheitskonzepte sowie Vorgaben zur Absicherung der Lieferkette. Diese Anforderungen gelten ausdrücklich auch für den OT-Bereich und unterstreichen dessen sicherheitsrelevante Bedeutung.

Wie OT-Security systematisch umgesetzt werden kann

Die ISA/IEC 62443 ist eine internationale Normenreihe, die speziell für die Sicherheit industrieller Automatisierungs- und Steuerungssysteme entwickelt wurde. Sie bietet einen umfassenden Rahmen für die Planung, Implementierung und den Betrieb von OT-Sicherheitsmaßnahmen.

Die Norm definiert klare Sicherheitsstandards und Best Practices und verfolgt einen **systematischen Ansatz**, um OT-Systeme wirksam abzusichern, zu überwachen und kontinuierlich weiterzuentwickeln.

Zugleich unterstützt sie Unternehmen dabei, die steigenden gesetzlichen Anforderungen aus **NIS2**, dem **Cyber Resilience Act (CRA)** sowie der Maschinenverordnung zu erfüllen. Darüber hinaus schafft sie die Grundlage für eine mögliche **Zertifizierung** nach international anerkannten OT-Sicherheitsstandards.

Die 3 Phasen der OT-Security*

Phase 1	Phase 2	Phase 3
Entdecken, Analysieren und Bewerten von Assets (Risikoanalyse**)	Entwickeln und Implementieren von Security-Maßnahmen	Überwachung, Instandhaltung sowie Reaktionen und Wiederherstellung nach Vorfällen

*siehe auch ISA/IEC 62443 2-1, ** siehe auch NIS2 Artikel 21

Risikomanagementmaßnahmen in der OT

Für eine ganzheitliche Umsetzung von Risikomanagementmaßnahmen in der OT sind die unten dargestellten Elemente entscheidend. Sie bilden die Grundlage, um dem **„Defense in Depth"-Ansatz** in der OT-Security gerecht zu werden.

Defense in Depth – auch als **Detection in Depth** bezeichnet – beschreibt die Implementierung mehrerer aufeinander abgestimmter Sicherheitsebenen, um Produktionsanlagen wirksam vor Bedrohungen zu schützen. Durch die Kombination verschiedener Maßnahmen wird das Risiko eines erfolgreichen Angriffs deutlich reduziert.

Dieser Ansatz umfasst **physische, logische** und **prozessbezogene** Sicherheitsmaßnahmen, die zusammen eine robuste und widerstandsfähige Sicherheitsarchitektur schaffen.

1. Strategie & Organisation

IT/OT-Sicherheitsstrategie & Governance
Festlegung von Richtlinien, Rollen und Verantwortlichkeiten.

Risikobewertung & Reviews
Regelmäßige Risikoanalysen, Bewertungen und Management-Reviews.

2. Inventarisierung & Bedrohungserkennung

IT/OT-Asset-Discovery & Management
Erfassung und Verwaltung aller Systeme, Geräte und Software.

Threat / Risk-Analysis
Analysieren und Bewerten von Assets (Risikoanalyse).

3. Präventive Schutzmaßnahmen

Endpoint Protection & Kontrolle
Antivirus, Host IDS/EDR, Datenschutzmaßnahmen, USB-Kontrolle.

Netzwerkarchitektur & Segmentierung
Trennung von IT- und OT-Netzen zur Minimierung von Angriffsflächen.

Identity & Access Management
Sicherstellung, dass nur autorisierte Personen Zugriff erhalten.

Sichere Fernzugriffe
Absicherung von Remote-Zugängen mit MFA und Verschlüsselung.

Supply Chain Security
Risikominimierung in Bezug auf SBOM, OEMs und Dienstleister.

4. Schwachstellenmanagement

Vulnerability Management & Patch Management
Erkennung, Priorisierung und Behebung von Sicherheitslücken.

Konfigurationshygiene
Standardisierte und sichere Konfiguration aller Systeme.

5. Notfallvorsorge & Reaktion

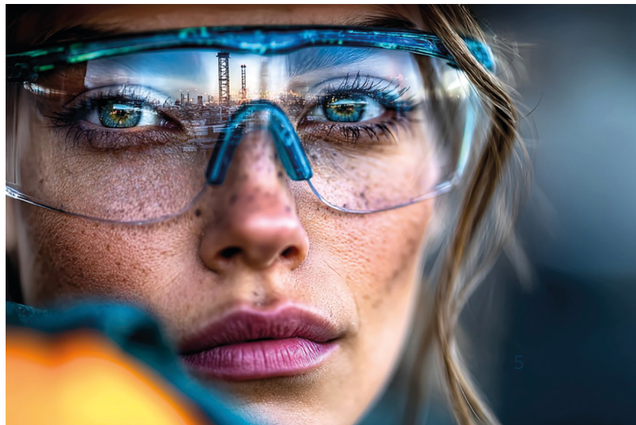
Backups & Wiederherstellung
Regelmäßige Datensicherungen, Test der Wiederherstellbarkeit.

Incident Response & Business Continuity Planning (BCP)
Vorgehenspläne für Sicherheitsvorfälle und Betriebsausfälle.

6. Kontinuierliche Verbesserung

Audits & Penetrationstests
Regelmäßige Überprüfung der Sicherheitsmaßnahmen.

Security Awareness & Schulungen
Sensibilisierung und Weiterbildung aller Mitarbeitenden.



Top 5 OT-Sicherheitsmaßnahmen nach IEC 62443 – in Prozessreihenfolge

1. Strategie & Organisation

Ziel: Grundlage für alle weiteren Maßnahmen schaffen.

Maßnahmen:

- IT/OT-Sicherheitsstrategie und Governance definieren.
- Rollen, Verantwortlichkeiten und Eskalationswege festlegen.
- Sicherheitsrichtlinien schriftlich dokumentieren.

Umsetzungstipp: Von Anfang an das **Management einbinden**, um Ressourcen, Budget und Entscheidungskompetenz zu sichern.

2. Risikoanalyse & Asset-Management

Ziel: Transparenz über Risiken und die zu schützenden Werte schaffen.

Maßnahmen:

- Inventarisierung aller OT-Assets (Hardware, Software, Netzwerke).
- Regelmäßige Risikoanalysen und Sicherheitsbewertungen.
- Kritikalität der Assets priorisieren.

Umsetzungstipp: Asset-Listen **automatisiert** erfassen, wo möglich – und regelmäßig mit der Realität abgleichen.

3. Technische Schutzmaßnahmen implementieren

Ziel: Angriffsflächen minimieren und Zugriff kontrollieren.

Maßnahmen:

- Netzwerksegmentierung zwischen IT und OT.
- Endpoint Protection (AV, EDR), Zugriffskontrollen, sichere Fernzugriffe (MFA, VPN). Lieferkettensicherheit (Prüfung von OEMs und Software-BOMs).

Umsetzungstipp: Nach dem Prinzip **“Least Privilege”** arbeiten – jeder Zugriff nur so weit wie unbedingt nötig.

4. Schwachstellen- & Patch-Management

Ziel: Sicherheitslücken zeitnah identifizieren und beheben.

Maßnahmen:

- Regelmäßige Schwachstellenscans und Konfigurationsprüfungen.
- Geplantes Patch-Management, auch für OT-spezifische Systeme.

Umsetzungstipp: Für OT-Systeme mit geringer Downtime-Toleranz **Patch-Testumgebungen** nutzen, bevor produktive Systeme aktualisiert werden.

5. Notfallvorsorge & kontinuierliche Verbesserung

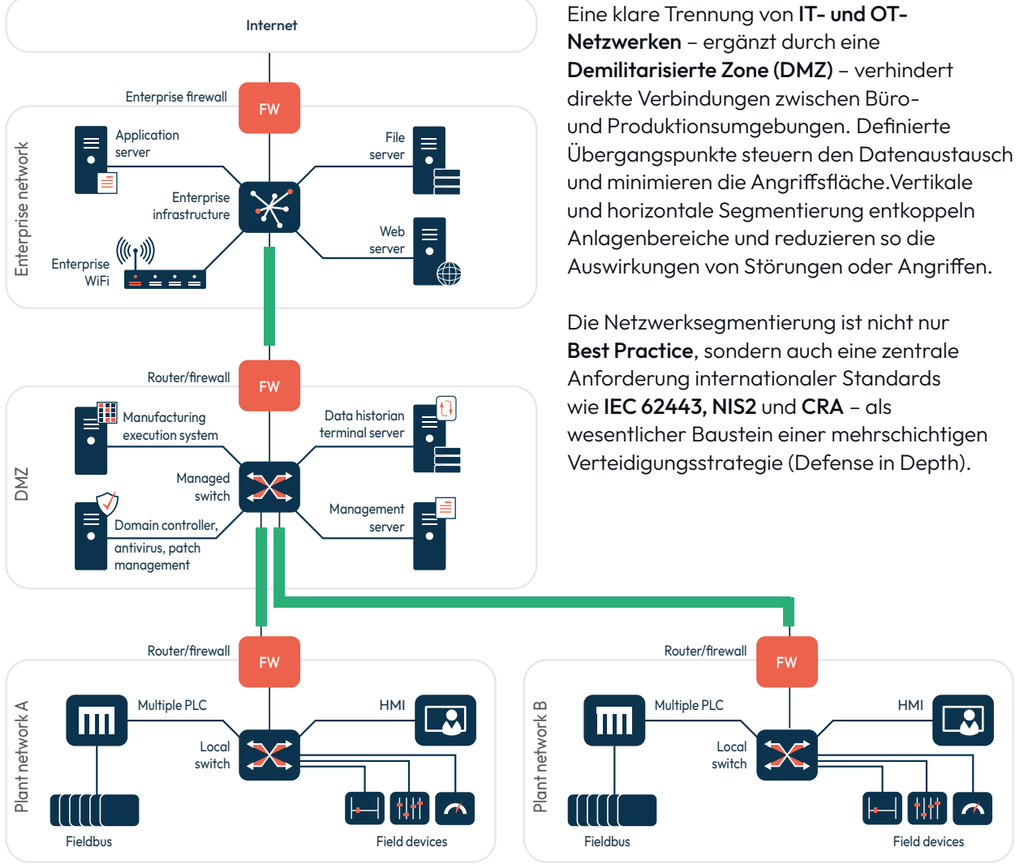
Ziel: Auf Sicherheitsvorfälle vorbereitet sein und aus ihnen lernen.

Maßnahmen:

- Incident-Response-Pläne und Business Continuity Planning (BCP).
- Backups erstellen und Wiederherstellung regelmäßig testen.
- Audits, Penetrationstests und Awareness-Trainings durchführen.

Umsetzungstipp: Notfallübungen mindestens einmal pro Jahr durchführen und die Ergebnisse in den Verbesserungsprozess zurückführen.

Risikominderung durch Netzwerksegmentierung



Eine klare Trennung von **IT- und OT-Netzwerken** – ergänzt durch eine **Demilitarisierte Zone (DMZ)** – verhindert direkte Verbindungen zwischen Büro- und Produktionsumgebungen. Definierte Übergangspunkte steuern den Datenaustausch und minimieren die Angriffsfläche.Vertikale und horizontale Segmentierung entkoppeln Anlagenbereiche und reduzieren so die Auswirkungen von Störungen oder Angriffen.

Die Netzwerksegmentierung ist nicht nur **Best Practice**, sondern auch eine zentrale Anforderung internationaler Standards wie **IEC 62443, NIS2** und **CRA** – als wesentlicher Baustein einer mehrschichtigen Verteidigungsstrategie (Defense in Depth).

OT-Security als ganzheitliches Portfolio

Als führender **Value-Added Distributor** im Bereich OT-Security unterstützt **Infinigate** Unternehmen mit einem **ganzheitlichen Ansatz**. Das Portfolio umfasst alle relevanten OT-Security-Bausteine, kombiniert mit gezieltem Know-how-Transfer sowie unterstützenden Services – von **OT-Engineering** bis hin zu **Finanzierungslösungen**.

	OT Use Cases (Kategorien)													
	Segmentation/Firewall	Network Infra Wired/Wireless	Remote Access	Network Access Control (NAC)	Virtualisation/Docker/VM	CPS Protection Platform	Asset Detection/Management	Vulnerability Management	Endpoint-Protection	Secure File Transfer	Security Inspection	Secure Media	Multi Factor Authentification (MFA)	Public Key Infrastructure (PKI)
Armis (Otorio)			✔			✔	✔	✔						
Barracuda	✔		✔		✔									
Belden-Hirschmann	✔	✔	✔		✔									
Belden-macmon				✔										
Check Point	✔		✔				✔		✔					
Cloudflare			✔											
Cybereason									✔					
Entrust													✔	✔
Extreme Networks		✔		✔										
Forcepoint	✔								✔					
Fortinet	✔	✔	✔	✔			✔		✔				✔	✔
Fortra			✔						✔	✔				
HPE aruba & Juniper Networks	✔	✔	✔	✔			✔							
Illumio	✔													
Microsoft						✔			✔				✔	✔
OneSpan													✔	
OPSWAT	✔		✔	✔		✔	✔	✔		✔	✔			
RUCKUS		✔												
SentinelOne									✔					
SonicWALL	✔	✔	✔						✔					
Sophos	✔	✔	✔						✔					
Swissbit												✔	✔	
Thales										✔			✔	✔
Trellix									✔					
TXOne	✔						✔		✔	✔	✔			
WatchGuard	✔		✔						✔					
Yubico													✔	

OT-Service Portfolio

Technical Services

Presales Beratung

Unsere Experten beantworten Ihre technischen oder architektonischen Fragen oder unterstützen Sie direkt bei Ihrem Kunden.

Direkter Endkunden-Support

Auf Wunsch supporten wir von Ihnen verkaufte Lösungen direkt bei Ihrem Endkunden, halten Sie in der Loop und sorgen für hohe Kundenzufriedenheit.

Demo / PoC Begleitung

Wir stellen Ihnen für Demo- und Evaluierungs-zwecke notwendige Testgeräte/Lizenzen in Projekten zur Verfügung. Auf Anforderung begleiten wir auch längere Testzeiträume (PoC).

Installation & Konfiguration

Wir unterstützen bei der reibungslosen Installation und Konfiguration neuer Lösungen oder übernehmen diese auch komplett. Eventuell auftretende Komplikationen und Fallstricke werden dabei kompetent vermieden.

Postsales Support

Für einen Großteil unseres Portfolios entlasten wir Ihre Technik-Abteilung durch schnellen, deutschsprachigen Support für von uns bezogene Lösungen.

Config Review / Systemoptimierung

Sie haben Sicherheitslösungen von Infinigate im Einsatz. Unsere Spezialisten unterstützen Sie bei der Prüfung der Konfiguration sowie deren weiterer Optimierung.

Training Services

Zertifizierungs-Trainings

Wir bilden Ihre Mitarbeiter aus, um die nötigen Zertifizierungen für Partnerprogramme zu erlangen.

Technische Workshops

Wenn Praxiswissen für Sie wichtiger als Zertifizierungen sein sollte, sind unsere technischen Workshops genau das richtige Format zum Wissensaufbau und -transfer für Ihre Techniker.

Sales

Neben den technischen Trainings veranstalten wir regelmäßig Vertriebstrainings und Webinare zu aktuellen Themen der IT/OT-Security.

Sales & Marketing Services

Telesales / Leadgenerierung

Aktionsbezogen oder auch dauerhaft generieren wir für Sie Endkunden-Leads oder unterstützen Sie bei der Kunden-Akquise für Events. Auf Wunsch in Ihrem Namen oder in Kombination mit einem unserer Hersteller.

Renewal-Support-Process

Wir sorgen für einen gut abstimmten Recurring Revenue-Process. Sie erhalten individuelle Renewal Angebote auf aktuellem Stand und Nachfolge SKU`s, wenn die initiale SKU nicht mehr verfügbar ist.

Marketing-Kampagnen

Wir helfen Ihnen bei der Definition und Umsetzung eines auf Ihre Bedürfnisse zugeschnittenen Lead to Cash Prozesses.

Events

Wir unterstützen Ihr Marketingteam bei der Organisation und Koordination eingebundener Hersteller. Weiterhin verfügen wir über ein weitreichendes Netzwerk von geeigneten Speakern zu diversen Themen.

Distribution Services

Lieferung & Logistik

Von der Direktlieferung an Ihre Kunden bis hin zu unserem Private-Labeling-Service, bei dem wir in Ihrem Namen den Endkunden direkt beliefern. Durch unsere hohe Lagerverfügbarkeit bieten wir für viele Produkte auch Versand am Bestelltag an.

Advanced-Hardware-Replacement (24X7X365)

Projektbezogen bieten wir erweiterte Austausch SLA`s an. Bis zu 24x7x365 innerhalb von 4 Std. in Deutschland. Auch international können wir SLA`s durch vor Ort Lagerhaltung eingehen.

Rollout Services Logistik & Export

Wir lagern in größeren Rollouts Ware für Sie ein um Lieferketten und Verfügbarkeit für Sie abzusichern. Auch internationale Direktlieferungen gehören zu unserem Leistungsumfang (siehe Financial-Services).

Automatisierung Ihrer Prozesse

Wir stellen Preislisten und Produktinformationen in verschiedenen Formaten und über Online Portale zur Verfügung. Ggf. kommt auch eine Anbindung an Ihre ERP-Systeme über API`s in Frage.

Rollout Services Konfiguration

Lassen Sie auf Wunsch Hardware vorkonfigurieren. Wir übernehmen OS sowie Firmware Changes, Einbau von Erweiterungen und vieles mehr, was oftmals nicht ab Werk vom Hersteller angeboten wird.

Partnerwelt und Shop

Die Infinigate Partnerwelt ist eine Plattform, auf der Sie als Partner Ihr Geschäft mit uns bequem organisieren und verwalten können: Im Shop können Sie die Produkte ausgewählter Hersteller direkt bestellen.

Channel Finance Services

Kreditlimits und Projektfinanzierung

Ob Verlängerung des Zahlungsziels, projektweise oder temporäre Erhöhung Ihres Kreditlimits bis hin zur offenen und stillen Zession. Diese Instrumente geben Ihnen maximale Flexibilität in Ihrem Geschäft.

Abwicklung in Fremdwährung

Vermeiden Sie Währungsrisiken oder unnötige Aufschläge durch die komplette Vertriebskette vom Endkunden über Reseller, Distributor bis zum Hersteller.

Vor-Finanzierung von Multi-Year Aufträgen

Sichern Sie sich die Top-Konditionen des Herstellers bei Mehrjahres-Bestellungen und / oder gewähren Sie Ihren Kunden die benötigten Zahlungsperioden (jährlich/ quartalsweise).

Internationales Geschäft

Wir unterstützen Sie mit unserem steuerlichen Know-how bei Auslandsgeschäften wie z.B. bei direkter innergemeinschaftlicher Lieferung sowie in Non-EU Länder. Hierbei übernehmen wir für Sie auf Wunsch auch die zolltechnische Vorbereitung sowie zur Absicherung den EMBARGO-Check.

Unsere Services im Detail finden Sie unter: www.infinigate.de/services

Logistik

+49 89 89048-100
logistik@infinigate.de

Trainings

+49 89 89048-401
akademie@infinigate.de

Professional Services

+49 89 89048-403
techservices@infinigate.de

Support

+49 89 89048-400
support@infinigate.de

Vertrieb

+49 89 89048-0
vertrieb@infinigate.de

Vereinbaren Sie gleich Ihr Beratungsgespräch

+49 89 89048-542

ot@infinigate.de

Infinigate Deutschland GmbH
Richard-Reitzner-Allee 8
85540 Haar/München

+49 89 89048-542
ot@infinigate.de
www.infinigate.com/de

infinigate
spark your growth

© Infinigate 11/25