infinigate
spark your growth

OT-Security

So schützen Sie relevante Infrastrukturen, Arbeitsumgebungen und Menschen

OT-Security – Sichern Sie Ihre Automatisierung und Steuerungen ab

OT-Security steht für „Operational Technology Security“ und bezieht sich auf die Praktiken und Technologien, die darauf abzielen, industrielle Kontrollsysteme (ICS), Prozesssteuerungssysteme und andere kritische Infrastrukturen vor Cyberbedrohungen zu schützen.

Im Gegensatz zur IT-Security, die sich auf Computernetzwerke und Daten konzentriert, konzentriert sich OT-Security auf die Sicherheit von physischen Geräten, Maschinen und Anlagen. Da viele dieser Systeme in der Vergangenheit nicht für den direkten Zugriff über das Internet (Fernwartung) entwickelt wurden und oft auf älteren Betriebssystemen (XP, Windows 7, etc.) basieren, können sie anfällig für Cyberangriffe sein.

OT-Security findet in folgenden Branchen Anwendung:

1. In der Fertigung wird OT angewandt, um Produktionsprozesse zu automatisieren und zu steuern, Maschinen und Anlagen zu überwachen und die Produktqualität zu gewährleisten.

2. Im Energiesektor umfasst OT die Steuerung und Überwachung von Kraftwerken, Stromnetzen und anderen Energieinfrastrukturen zur Erzeugung, Übertragung und Verteilung von Strom und anderen Energiequellen.

3. In der Wasser- und Abwasserwirtschaft wird OT eingesetzt, um Wasseraufbereitungsanlagen, Pumpstationen und Verteilungssysteme zu steuern und zu überwachen, um eine zuverlässige Wasserversorgung und Abwasserentsorgung sicherzustellen.

4. Im Transportwesen umfasst OT die Steuerung und Überwachung von Verkehrssignalen, Schienen- und Straßenverkehrssystemen, Flughäfen und anderen Transportinfrastrukturen zur Sicherstellung eines sicheren und effizienten Personen- und Warentransports.

5. Im Gesundheitswesen wird OT für die Steuerung und Überwachung von medizinischen Geräten, Patientenüberwachungssystemen & Krankenhausinfrastrukturen eingesetzt, um die Patientenversorgung und -sicherheit zu verbessern.

Eine funktionierende OT-Infrastruktur ist aus folgenden Gründen wichtig:

1. Betriebsunterbrechungen und Produktionsstillstände bringen enorme finanzielle Risiken, wie Umsatzverluste sowie Instandsetzungskosten mit sich und beschädigen das Ansehen des Unternehmens.

2. Ausfall von OT-Systemen können die physische Sicherheit von Mitarbeitern, der breiten Öffentlichkeit und der Umwelt gefährden.

3. Neben den physischen Auswirkungen können Cyberangriffe auf OT-Systeme zum Diebstahl sensibler Daten führen oder dazu genutzt werden, Abläufe zu sabotieren. Dies kann zu langfristigen Sicherheitsproblemen und Wettbewerbsnachteilen für betroffene Unternehmen führen.

Insbesondere die ab 2024 in Europa relevanten Gesetze **NIS2** und der **Cybersecurity Resilience Act (CRA)** spielen für die OT-Security eine entscheidende Rolle, indem sie die Sicherheitsanforderungen und -standards für Betreiber wesentlicher und wichtiger Unternehmen, Anlagen- und Maschinenbauer sowie Dienstleister massiv erhöhen.

Dabei beziehen sich die in den Gesetzen geforderten Risikomanagementmaßnahmen wie Risikoanalyse- und Sicher-heitskonzepte sowie Gewährleistung der Sicherheit in der Lieferkette auch auf die OT-Security.

Sie haben Fragen zu NIS2 und CRA?

Fordern Sie unsere Broschüre an.

scnem2.com/a.php?sid=6ehgy.bm6m74,f=7

Wie OT-Security systematisch umgesetzt werden kann

Die Norm ISA/IEC 62443 ist eine internationale Normenreihe, die speziell für die Sicherheit von industriellen Automatisierungs- und Steuerungssystemen entwickelt wurde. Sie bietet einen umfassenden Rahmen für die Implementierung von OT-Sicherheitsmaßnahmen und -verfahren. Sie definiert klare Sicherheitsstandards und Best Practices für die Planung, Implementierung und den Betrieb von OT-Security Maßnahmen.

Die Norm legt einen systematischen Ansatz zur Umsetzung von Sicherheits-maßnahmen fest, der allen Beteiligten dabei hilft, ihre OT-Systeme effektiv zu verbessern, zu überwachen und kontinuierlich zu warten.

Diese Systematik trägt im gleichen Zug dazu bei, den gesetzlichen Anforderungen aus NIS2 und CRA zu entsprechen und bietet den Ausblick sich entsprechend nach der Norm zertifizieren zu lassen.

Die 3 Phasen der OT-Security*

Phase 1 ▶ **Phase 2** ▶ **Phase 3**

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

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

Die OT-Security Bausteine

Für eine umfassende Umsetzung von Risikomanagementmaßnahmen in der OT, sind die folgenden abgebildeten Elemente erforderlich. Sie sind elementar, um dem „Defense in depth“ Ansatz in der OT-Security gerecht zu werden. „Defense/ Detection in depth“ bedeutet, entsprechende Sicherheitsebenen zu implementieren, um eine Produktion vor Bedrohungen zu schützen. Durch Kombination verschiedener Maßnahmen wird das Risiko eines erfolgreichen Angriffs verringert. Dieser Ansatz umfasst physische, logische und prozessbezogene Sicherheitsmaßnahmen, die zusammen eine robuste Sicherheitsarchitektur bilden.

Risikoanalysen, Bewertungen und Reviews	IT/OT Asset Discovery, Management & Threat Detection (Auswahl, Implementie-rung und Betrieb)	Endpoint Protection & Kontrolle (AV, Host IDS/EDR, Data Protection, USB Kontrolle)	Monitoring & Threat Intelligence
Mitarbeiter Ausbildung & Awareness	Sichere Fernzugriffe	Vulnerability Management, Konfigurationshygiene & Patch Management	BackUps, Incident Response, Recovery und Business Continuity Planing (BCP)
Netzwerk Architektur & Segmentierung (IT/OT)	Identity & Access Management und Control	Supply Chain Security (Risikominimierung hinsichtlich (S) BOM, OEMs und Dienstleistern)	Audits, Pen-Tests und kontinuierlicher Verbesserungsprozess
IT/OT Security Geschäftspolitik & Organisation			

Beispiele und Hintergründe einer 5-stufigen Umsetzung von OT-Security-Bausteinen

1 Netzwerk Architektur & Segmentierung (IT/OT)

- IT-OT-DMZ-Makro-Segmentierung mittels zweier Schichten physischer Firewalls.
- Festlegung eines restriktiven Datenflusses von OT an IT, nicht umgekehrt.
- Fortführung Netzwerk-Mikro-Segmentierung basierend auf Zonen und Leitungen.

2 Bestandsaufnahme und Kontrolle von Assets**

- Zielsetzung ist ALLE schützenswerte Assets, welche sich im Netzwerk befinden zu kennen, was gerade in historisch gewachsenen Produktionsnetzwerken von elementarer Bedeutung ist.
- Ein Asset Management ist Kernbestandteil moderner IACS/OT-Netzwerke - und wird in der NIS2 gefordert!
- Auch wenn Assets nicht zu 100% erfasst wurden, ist jeder hohe Wert ein guter Ausgangspunkt.
- Asset Management muss sich auf dem neuesten Stand befinden, ist es nicht oder existiert es nicht, sollte damit umgehend begonnen werden!

3 Incident-Response-Planung

- Die Fähigkeit auf einen auf einen Vorfall in der Produktion mittels Ablaufplan organisiert reagieren zu können.
- Kernpunkte u.a.:
    - Sicherheit Menschen
    - Welche Stellen werden um Hilfe gerufen?
      Welche Behörden informiert werden?
    - Schnelle Wiederherstellung der Funktionalität der SPS
    - Schnelle Wiederinbetriebnahme von Assets (Anlagen und Maschinen) und der Produktion

4 Backup & Wiederherstellung

- Baut auf der oben beschriebenen Incident-Response-Planung auf
- Kernpunkte u.a.:
    - Örtlichkeit Backups (inner-/außerbetrieblich)
    - Vollständigkeit der Backups bezogen auf Assets
    - Wiederherstellungsdauer Assets
    - Testwiederherstellungen der Backups vorab
    - Dokumentierte Anweisungen zur Wiederherstellung

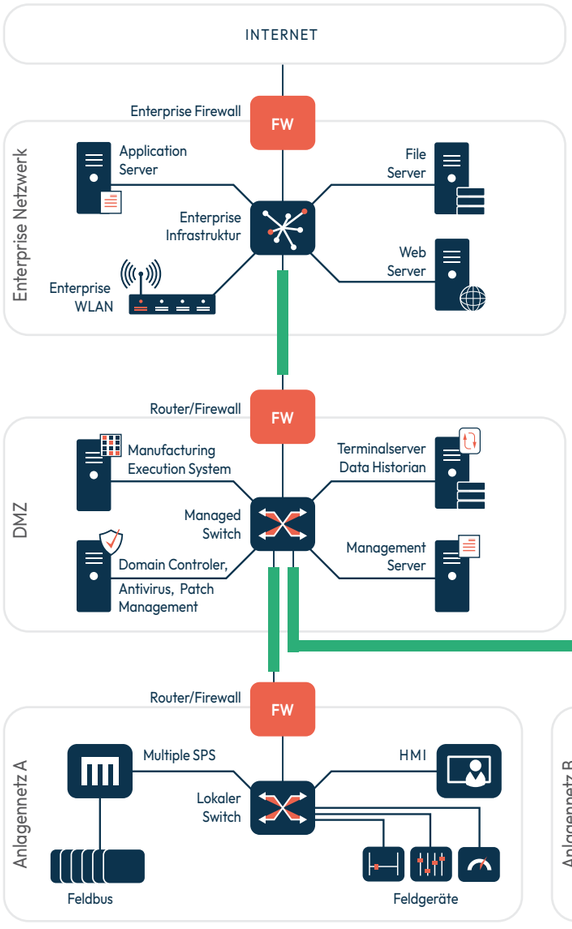
** siehe auch NIS2 Artikel 21

5 Kontinuierliches Schwachstellenmanagement

- Schwachstellenmanagement in ICS/OT funktioniert anders als in IT.
- Erfordert zwingend eine Bestandsaufnahme (siehe #2) für
- Kernpunkte u.a.:
    - Identifizierung aktueller Schwachstellen
    - Klassifizierung des Risikos seitens des Herstellers
    - Riskoanalyse hinsichtlich Bedrohung und Konsequenzen

Risikominderung durch Netzwerksegmentierung

Die folgende Abbildung zeigt eine Netzwerkarchitektur, die in vier Zonen unterteilt ist:



Enterprise Zone für Bürobetrieb, eine demilitarisierte Zone (DMZ) für die Kommunikation zwischen Enterprise- und Anlagennetzen, wobei direkte Kommunikation zwischen Enterprise- und Anlagennetzen ausgeschlossen ist. Die grünen Zonenübergänge dienen als Kommunikationskanäle zwischen den Segmenten.

Die Architektur ist sowohl vertikal als auch horizontal segmentiert, um unabhängige Anlagenbereiche (A/B) zu entkoppeln und die Auswirkungen von Störfällen zu minimieren.
Dies schützt nicht nur vor böswilligen Angriffen, sondern reduziert auch die Folgen normaler Störungen.

OT-Security ganzheitlich gedacht – in jeder Phase

Die Infinigate unterstützt als führende Added Value Distribution in der OT-Security mittels einer ganzheitlichen Betrachtung und entsprechenden Leistungen. Angefangen bei den relevanten OT-Security-Bausteinen, dem Know-how-Transfer als auch unterstützenden Services wie OT-Engineering und Finanzierungs-Services.

	Netzwerk Architektur & Segmentierung	IT/OT Asset Discovery & Threat Detection	Endpoint Protection	Monitoring & Threat Intelligence	Sichere Fernzugriffe	Vulnerability Management, Patch Management	Incident Response	Identity & Access Management und Control	Supply Chain Security
ARMIS		✔		✔	✔	✔	✔		
Barracuda Your journey, secured.	✔				✔	✔	✔	✔	
CHECK POINT	✔	✔	✔	✔	✔		✔		✔
FORTINET	✔	✔	✔	✔	✔	✔	✔	✔	✔
HPE aruba networking	✔	✔			✔	✔		✔	
kaspersky	✔	✔	✔	✔		✔	✔		✔
Belden | macmon	✔	✔			✔			✔	
SOPHOS	✔		✔	✔	✔			✔	
THALES Building a future we can all trust								✔	
txOne networks	✔	✔	✔	✔	✔	✔	✔		✔

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 Evaluierungszwecke 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

Ihr OT-Expertenteam bei Infinigate Deutschland

Head of OT

Patrick Scholl

Business Delevopment Manager OT

Andreas Danöhl

Business Delevopment Manager OT

Alexander Gebhard

System Engineer OT

Florian Loock

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.de

infinigate
spark your growth