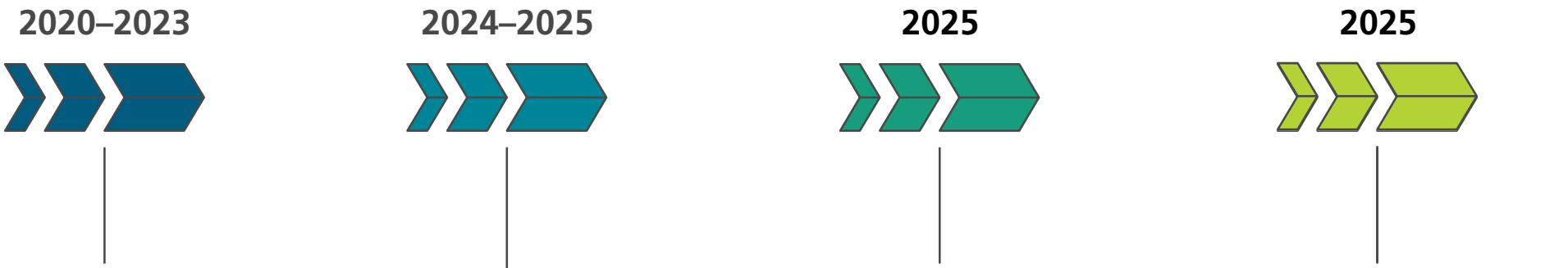
Neue Veröffentlichungen im Bereich OT-Assetmanagement

Fraunhofer IAO

Arbeiten zu OT-Assetmanagement

Aufmerksamkeit von öffentlichen Stellen zu OT-Assetmanagement

Das Thema Assetmanagement in der OT wurde Langezeit als ein Nischenthema betrachtet und hat dementsprechend wenig Aufmerksamkeit von öffentlichen Stellen bekommen. Seit 2020 bekommt das Thema aber langsam mehr Beachtung.



Schlüsselaspekte in der Übersicht

CISA

Asset-Inventory
Basis jeder OT-Sicherheitsmaßnahme; ohne Inventar keine Risikobewertung oder Segmentierung möglich

Asset-Kategorisierung
Beschreibt konkrete Schritte zur Erfassung von OT-Assets (Identifikation, Kategorisierung, Attributmodell).

Standardisierte Taxonomie
Verwendung einer konsistenten Sprache zur Beschreibung von Assets.

Kontinuierliche Pflege
Aufrechterhaltung und Aktualisierung des Inventars im Laufe der Zeit.

Was ist ein OT-Asset-Inventory?

OT-Assetmanagement CISA

Das OT-Assetmanagement ist das Fundament für viele Management-Prozesse, darunter auch das Risikomanagement, Schwachstellenmanagement und das Patchmanagement, denn du kannst nur das schützen, was du kennst.

Kernaussagen

- Ohne vollständiges Asset-Inventory ist OT-Sicherheit nicht umsetzbar. Es bildet die Grundlage für Risikoanalysen, Segmentierung, Monitoring und Incident Response.
- Inventare müssen Struktur und Kontext enthalten, nicht nur Gerätelisten. Dazu gehören Typ, Funktion, Konnektivität, Kommunikationsbeziehungen und kritische Abhängigkeiten.
- Das Inventar muss aktuell gehalten werden und darf kein „Einmal-Projekt“ sein. Die Dokumente betonen fortlaufende Pflege als Prozess mit klaren Verantwortlichkeiten.
- Ein zuverlässiges Inventar ermöglicht fundierte Betriebs- und Sicherheitsentscheidungen. Es reduziert Unsicherheiten bei Änderungen, Störungen und Krisenlagen.


TLP:CLEAR

Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators

Publication: August 13, 2025

U.S. Cybersecurity and Infrastructure Security Agency
U.S. Environmental Protection Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
Germany's Federal Office for Information Security
Netherlands' National Cyber Security Centre
New Zealand's National Cyber Security Centre

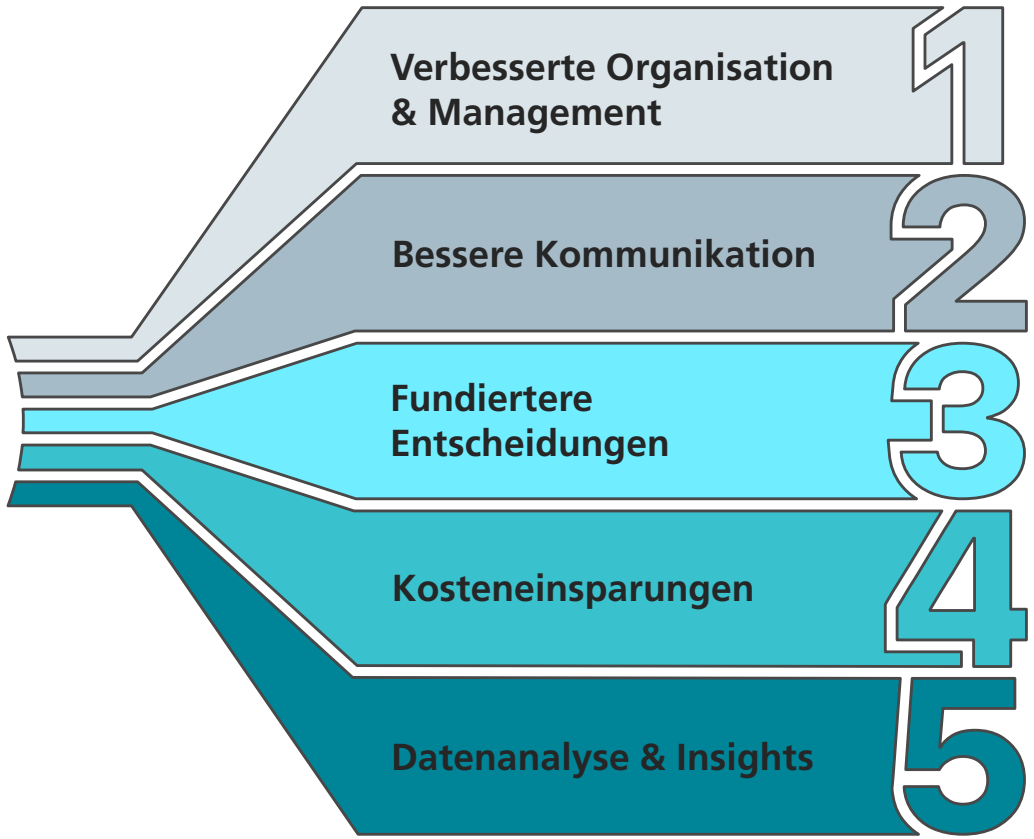
This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see Traffic Light Protocol (TLP) Definitions and Usage.

TLP:CLEAR

➢ Link zum Dokument: Asset Inventory

Welchen Nutzen hat OT-Taxonomie?

OT-Assetmanagement CISA



Eine gut strukturierte OT-Taxonomie ermöglicht die effiziente Kategorisierung von Assets, Prozessen und Daten, was das Management vereinfacht und die Abläufe effizienter macht.

Einheitliche Terminologie und Klassifikationen sorgen dafür, dass alle dieselbe „Sprache“ sprechen. Missverständnisse werden reduziert und die Zusammenarbeit zwischen Teams verbessert.

Klare Übersicht über Abhängigkeiten und Beziehungen zwischen Assets und Prozessen unterstützt informierte Entscheidungen, z. B. bei Ressourcenplanung, Wartung oder Upgrades.

Optimiertes Assetmanagement reduziert Ineffizienzen, minimiert Ausfallzeiten und steigert die betriebliche Effizienz.

Eine strukturierte Taxonomie bietet eine klare Basis für Datenanalyse, liefert wertvolle Erkenntnisse und unterstützt kontinuierliche Verbesserung und Innovation.

OT-Asset-Inventory und Taxonomie Schritt für Schritt

OT-Assetmanagement CISA

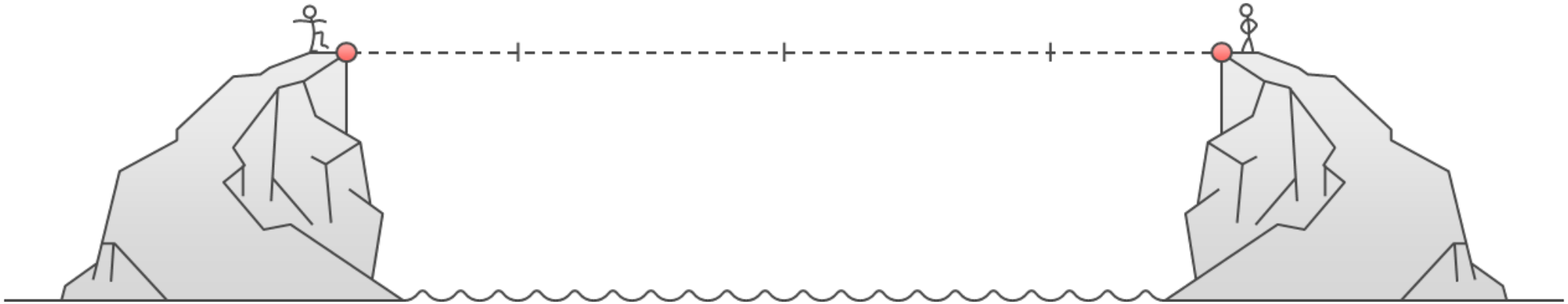
1) Ziele und Umfang definieren

2) Assets identifizieren und Attribute sammeln

3) Erstellen einer Taxonomie zur Kategorisierung von Assets

4) Verwalten und Sammeln von Daten

5) Lebenszyklus Managen



Schritt 1: Ziele und Umfang definieren

OT-Assetmanagement CISA

- **Wo wollen wir hin?** Was ist der Motivator hinter dem Projekt und womit fangen wir an? Konkretes, erreichbares Ziel definieren.
- **Wer sind die Stakeholder?** Wer ist in dem Projekt involviert und wer hat welche Rolle? Wer sind die Ansprechpartner, wer sammelt die Daten und wer Organisiert?
- **Was ist die Scope?** Was soll alles erfasst werden? Was ist ein Asset? Fokussiert sich die Projekte auf bestimmte Bereiche oder Werke?

Tipps

1) Holt die Stakeholder mit ins Boot. Was für Attribute sind für die wichtig?
2) Konkrete und erreichbare Ziele setzen. Mit Piloten anfangen.
3) Zeitrahmen setzen.

Schritt 2: Assets identifizieren und Attribute Sammeln

OT-Assetmanagement CISA

1

Assets Identifizieren

Durchführen einer Physische und Logische Inspektion um Assets zu Identifizieren. Gibt es Tools, die dafür verwendet werden können? Können Netzwerkscans durchgeführt werden? Gibt es bereits Dokumentation oder geführte Listen von Assets die gesammelt und aggregiert werden können?

2

Asset Attribute sammeln

Welche Attribute müssen gesammelt werden? Die wichtigsten sollten priorisiert werden. Darunter unter anderem IP-Adresse, Ports, OS, Kritikalität des Assets, Hostname, Accounts, Hersteller, Model, Standort, ….

3

Wiederholbar gestalten

Das Asset-Inventory verändert sich ständig und muss aktuell gehalten werden.

Schritt 3: Erstellen einer Taxonomie zur Kategorisierung von Assets

OT-Assetmanagement CISA

- **Klassifizieren von Assets:** Wie sollen Assets klassifiziert werden? Nach Kritikalität für die Organisation? Nach Funktion?
- **Kategorisieren von Assets:** Wie sollen Assets Kategorisiert werden? Nach Zonen für Sicherheitsanforderungen? Nach Netzwerken und Kommunikationsknotenpunkten?
- **Organisieren von Assets:** Wie hängen die Assets zusammen? Was gibt es für Abhängigkeiten? Wer ist verantwortlich für das Asset? Wie werden Assets bezeichnet und Nummeriert?

Schritt 4: Verwalten und Sammeln von Daten

OT-Assetmanagement CISA

- **Weitere Datenquellen miteinbeziehen:** Neben den bereits genannten Datenquellen für Asset-Informationen kann es weitere Datenquellen geben die wertvollen und ergänzenden Informationen über Assets beinhalten können. Beispielsweise Informationen des Herstellers durch SBOM's/IBOM's, Handbücher und weiteres.
- **Daten Speichern und sichern:** Ein voll funktionsfähiges Assetmanagement verfügt in der Regel über eine Zentralisierte Datenbank die als Single Source of Truth fungiert in der die Asset Informationen zusammenfließen. Diese Informationen repräsentieren das Fundament der Organisation und können auch für Angreifer sehr interessant sein. Daher sollten sie auch entsprechend gut Geschützt werden.

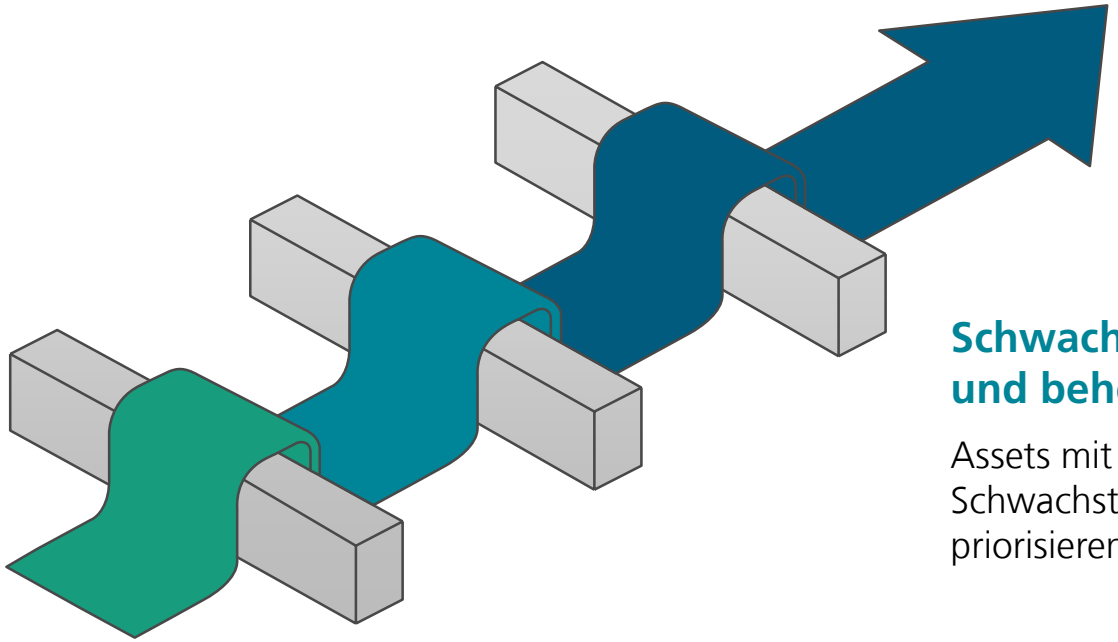
Schritt 5: Lebenszyklus Managen

OT-Assetmanagement CISA

- **Lebenszyklus Zustände definieren:** Definieren der Lebenszyklus zustände der Assets. Beispielsweise Beschaffung, Onboarding, Betrieb, Wartung, Offboarding und Außerbetriebnahme.
- **Entwickeln von Lebenszyklus Richtlinien:** Definieren von Richtlinien für Wartung, Austausch und Backups definieren. Zustandsübergänge für den Lebenszyklus definieren und Change-Management Prozesse anwenden. Inventar immer aktuell halten.

Wie geht es nach der Inventarisierung weiter? (I)

OT-Assetmanagement CISA



Optimieren der Sicherheitslage

Integrieren von Threat Intelligence und Sicherheitsarchitektur wie Segmentierung

Schwachstellen managen und beheben

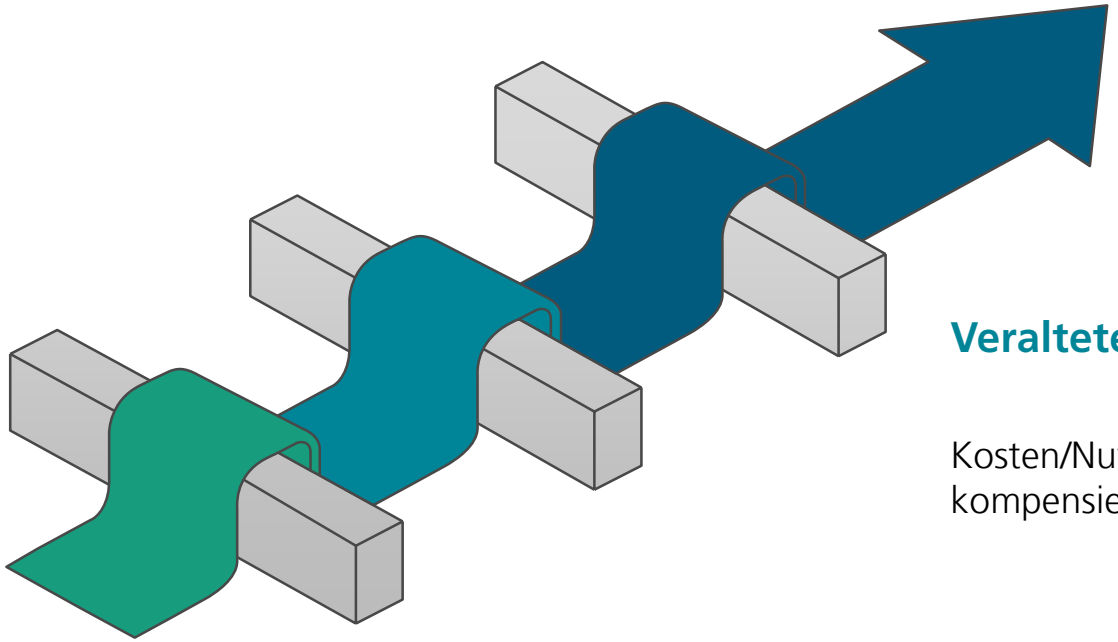
Assets mit Schwachstellendatenbanken abgleichen. Kritische Schwachstellen Identifizieren und deren Behebung priorisieren.

Härten

Bekannte Schwachstellen mit Patches und Updates beheben. Assets härten und gegeben falls nach Hersteller Empfehlung verwalten.

Wie geht es nach der Inventarisierung weiter? (II)

OT-Assetmanagement CISA



Redundanz erstellen

Ersatzteillager prüfen: Sind kritische OT-Assets ausreichend abgedeckt?

Veraltete Systeme ersetzen

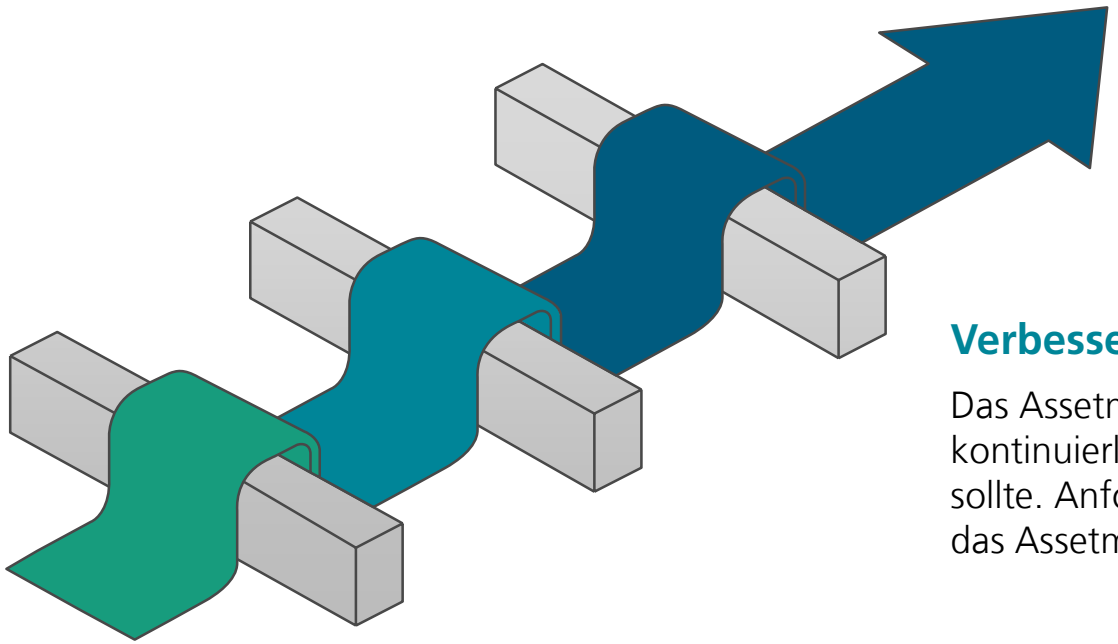
Kosten/Nutzen abwägen: Downtime vs. Austausch vs. kompensierende Kontrollen.

Wartungszyklus anpassen

Wartungspläne regelmäßig prüfen. Schwachstellen und Mitigationsmaßnahmen berücksichtigen. Patches während der Wartungsfenster durchführen. Auf Ausnahmen im Notfall vorbereiten.

Wie geht es nach der Inventarisierung weiter? (III)

OT-Assetmanagement CISA



Performanz messen

Kontinuierliche Messung der Performanz und weiterer Variablen wie Temperatur, Druck usw. Zur frühzeitigen Erkennung von Wartungsproblemen.

Verbesserungen

Das Assetmanagement ist ein lebender Prozess der kontinuierlich verbessert oder zumindest aktuell gehalten sollte. Anforderungen können sich mit der Zeit ändern und das Assetmanagement muss sich dem anpassen können.

Mitarbeitende schulen

Das Asset Inventory und das Management drum herum muss verwaltet und gepflegt werden. Dafür sollten Ressourcen verfügbar gemacht werden. Außerdem sollte das Bewusstsein über die Relevant des Assetmanagement bei Relevanten Stakeholder gefördert werden.

Schlüsselaspekte in der Übersicht

NCSC

Zuverlässige Darstellung
Ziel ist eine zuverlässige, vollständige und aktuelle Darstellung der OT-Umgebung (Single Source of Truth).

Architekturverständnis
Das OT-Assetmanagement ist nicht nur eine Inventarliste, sondern auch eine Darstellung der Architektur und Umgebung der Organisation.

Klare Verantwortung
Für ein funktionierendes OT-Assetmanagement ist eine klare Verantwortung unverzichtbar.

Informationsschutz
Informationen über das OT-Assetmanagement sind essenziell für ein funktionierendes Incident Response und Risikomanagement und müssen entsprechend geschützt werden.

Priorisieren nach Kriterien

OT-Assetmanagement NCSC

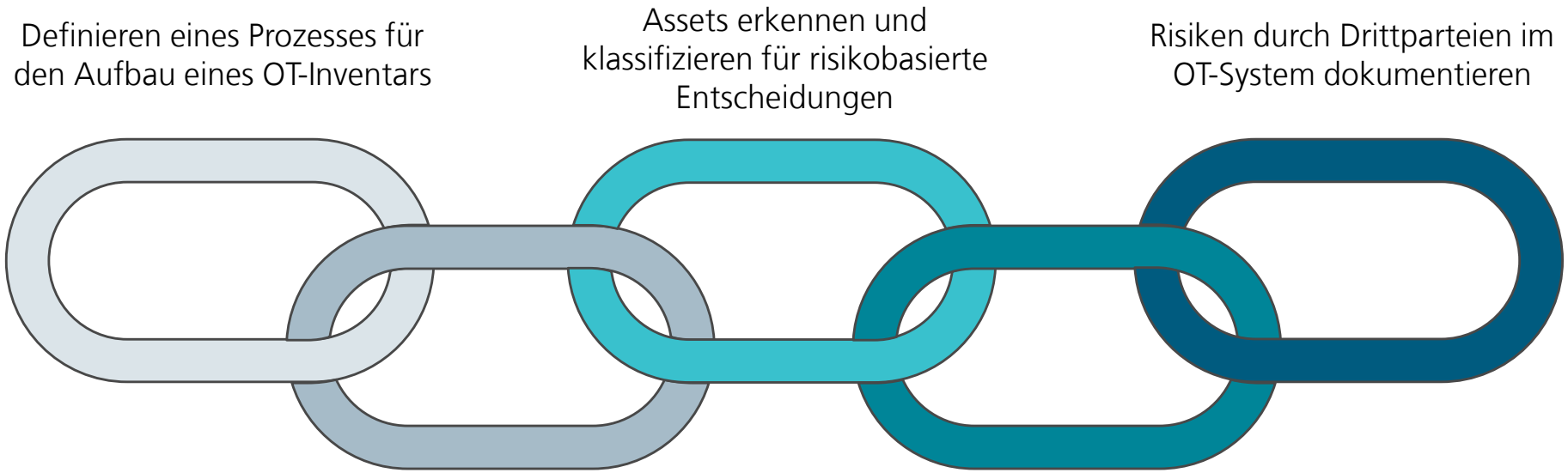
Organisationen sollten es sich zum Ziel setzen eine vollständige Abbildung aller ihrer OT-Systeme zu erstellen. Dafür sollten folgende Kriterien priorisiert werden:

- **Auswirkung auf den Geschäftsbetrieb** oder potenzielle **nationale Auswirkungen**.
- **Verbindungen zu Drittparteien**, insbesondere wenn diese die Systemkonfiguration ändern oder direkten Einfluss auf den Prozess nehmen können.
- **Gesamte Exposition** des Systems, unter Berücksichtigung der Anzahl an Verbindungen zu externen Diensten, bei denen Ihre Organisation die Sicherheitskontrollen nicht selbst festlegt.

➢ Link zum Dokument: OT-System Abbildung

Fünf Prinzipien für das OT-Assetmanagement

OT-Assetmanagement NCSC



Prinzip 1: Definieren eines Prozesses für den Aufbau eines OT-Inventars

OT-Assetmanagement NCSC

National Cyber Security Centre
a part of GCHQ

Wie werden Informationen gesammelt?

- Definieren, welche Daten benötigt werden (Assets, Funktionen, Standorte, Schnittstellen).
- Festlegen der Quellen: Inventuren, Dokumentation, Netzwerkscans, Expertenwissen.

Wie werden Informationen validiert?

- Qualität prüfen: Vollständigkeit, Korrektheit, Konsistenz.
- Verantwortliche für Validierung benennen und Prozess definieren.

Wie wird das definitive Inventar gepflegt?

- Change-Management implementieren.
- Änderungen dokumentieren und Verantwortlichkeiten klar definieren.

Tipps

1) Identifizieren von Informationslücken
2) Zeitplan für aktives Scannen definieren damit Angreifer Scans nicht untergehen.
3) Gegeben falls mehrere Quellen zur Validierung vergleichen.
4) Change-Management zur Verwaltung der Lebenszyklus Übergänge

Prinzip 2: Aufbau eines OT-Informationssicherheits-Managementprogramms

OT-Assetmanagement NCSC

National Cyber Security Centre
a part of GCHQ

Scope des Programms definieren – „What is in scope?“

- Übersicht aller relevanten OT-Informationen erstellen: Design Informationen, Business Informationen, Authentifizierungsinformationen, Betriebsdaten, Risikobewertungen.

Wert der Informationen für Angreifer – „What is the value to an attacker?“

- Angreifer benötigen Informationen, um OT-Systeme zu stören oder zu sabotieren
- Aggregation von Informationen erhöht Risiko („latent intelligence“)

Sicherheitsmaßnahmen – „What security considerations?“

- Schutz aller OT-Informationen entsprechend Vertraulichkeit, Integrität und Verfügbarkeit (CIA-Triad)

Prinzip 3: Assets erkennen und klassifizieren für risikobasierte Entscheidungen

OT-Assetmanagement NCSC

National Cyber Security Centre
a part of GCHQ

Kritikalität

- Wie kritisch ist das Asset für den Betrieb?
- Ist das Asset Relevant für die Sicherheit der Mitarbeiter?
- Ist das Asset Relevant für die Cybersicherheit?

Exposition

- Wie, Wann und Wo kann auf das Asset zugegriffen werden?
- Was kann mit dem Asset Kommunizieren?
- Ist das Asset öffentlich (über das Internet) erreichbar?

Verfügbarkeit

- Wie verfügbar muss das Asset sein?
- Ist eine Downtime zur Wartung für das Asset vorgesehen?

Prinzip 4: Verbindungen innerhalb des OT-Systems dokumentieren

OT-Assetmanagement NCSC

National Cyber Security Centre
a part of GCHQ

1) Mit welchen Systemen/Assets muss das Asset kommunizieren?

Einheitliche und sichere Datenaustauschmöglichkeiten sollten wann immer möglich verwendet werden. Weiterhin müssen die Informationsklassifizierungsregeln beachtet und durchgesetzt werden.

2) Welche Kommunikationsprotokolle werden verwendet und wie werden sie gesichert?

CIA-Dreieck. Welche Legacy Systeme und Protokolle werden verwendet und warum?

5) Könnte ein Kompromiss bestehende Kontrollen umgehen?

Was kann passieren wenn ein Netzwerk oder eine Verbindung Kompromittiert wird?

3) Welche Architektur basierten Sicherheitskontrollen existieren bereits?

Netzwerk Kontrolle und Monitoring. Zugriffskontrolle. Netzwerk Segmentierung. Isolierung ….

4) Welche Netzwerkeinschränkungen bestehen?

Bandbreite, Latenz und Redundanz

Prinzip 5: Risiken durch Drittparteien im OT-System dokumentieren

OT-Assetmanagement NCSC

National Cyber Security Centre
a part of GCHQ

Verbindungen und Vertrauensstufen

- Detaillierte Übersicht aller externen Verbindungen
  - High Trust: Gleichwertige CNI-Systeme
  - Partial Trust: Unternehmensnetzwerke
  - Low Trust: Drittanbieter, Integratoren, MSPs
- „Browse-Down"-Prinzip: höhere Vertrauensstufen verwalten niedrigere

Vertragliche Anforderungen

- Drittanbieter-Verträge können Zugriff und Sicherheitskontrollen beeinflussen
- Einschränkungen minimieren, wo möglich
- Kompensationsmaßnahmen dokumentieren (z. B. Monitoring, Netzwerksegmentierung)

Out-of-Band-Zugriffe prüfen

- Drittanbieterinstallationen auf unkontrollierte Zugänge prüfen
- Risiken bewerten, dokumentieren und absichern; wenn möglich entfernen

CISA und NCSC im Vergleich

Fazit

CISA

- Entwicklung einer OT-Taxonomie zur Strukturierung von Assets
- Schrittweiser Aufbau des Inventars
- Managen des Lebenszyklus ist ein integraler Bestandteil
- Beziehungen und Abhängigkeiten zwischen Assets

NCSC

- Assetinformationen als Unterstützung für Risikoentscheidungen
- Assetinformationen müssen geschützt werden
- Risiken durch Lieferanten und Dritte

CISA und NCSC

- Das Assetinventar ist das Fundament und muss aktuell gehalten werden. Es verfügt über Kritische und schützenswerte Daten
- Priorisierung anhand Kritikalität
- Systematische Identifikation und Kategorisierung

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

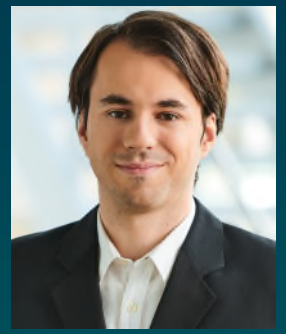
Lernlabor Cybersicherheit

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
  - Empathisches 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



Matthias Winterstetter

Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO

matthias.winterstetter@iao.fraunhofer.de

+49 152 22543931