FINSOZ e.V.
Digitalverband Sozialwirtschaft

FINSOZ e.V.

Die Operational Technology-Guideline

Gebäudemanagement

ein (weiteres) Einfallstor für Cyberangriffe

1. Auflage, Oktober 2023

www.finsoz.de

Gebäudemanagement – ein (weiteres) Einfallstor für Cyberangriffe

Die Operational Technology-Guideline

Herausgeber: FINSOZ e.V.

Fachgruppe IT-Compliance

Oktober 2023

Vorwort

Es lässt sich eine Zunahme von Angriffen an der Schnittstelle von „Information Technology“ (IT) und „Operational Technology“ (OT) beobachten. Das erfordert nicht nur eine nachhaltige Sicherheitsstrategie, sondern überhaupt eine Auseinandersetzung mit dem wachsenden Einfluss von vernetzten Geräten und Anlagen aller Art.

Dieses Dokument legt bewusst den Kontext auf „Operational Technology“ in der Sozialwirtschaft. Die Erkenntnisse lassen sich gut auf andere Branchen übertragen, zum Beispiel das Gesundheitswesen. Ganz bewusst wurde aber ein weitergehender Kontext eines produzierenden Unternehmens (inklusive Sensorik oder Robotik) nicht betrachtet.

Wir wünschen den Leserinnen und Lesern dieser Lektüre viele gute Anregungen und Anstöße für kritische Denkprozesse zur IT- und OT-Sicherheit in der eigenen Organisation.

Fachgruppe IT-Compliance, im Juni 2023

Autoren und Mitwirkende:

Thomas Althammer	Althammer & Kill GmbH & Co. KG
Alexander Gottwald	Solidaris Unternehmensgruppe
Michaela Grundmeier	Caritas Seniorenheime Betriebsführungs- und Trägerschaft GmbH Vorständin FINSOZ e.V.
Markus Hemgesberg	Diakonie Michaelshoven e.V.
Christian Lax	Alida Schmidt-Stiftung
Martin Lembcke	Diakoniestiftung in Sachsen Stiftung bürgerlichen Rechts
Alexander Overmann	Connext Communication GmbH
Wolfgang Paris	Rummelsberger Dienste für Menschen gemeinnützige GmbH
Jürgen Prummer	d.velop AG
Dorothee Steckel	Stiftung Nieder-Ramstädter Diakonie
Anja Thorwesten	Caritasverband für das Erzbistum Paderborn e.V.

Inhalt

Gender-Hinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

1. Einleitung und Management Summary

Was hat die Sozialwirtschaft mit „Operational Technology“ zu tun? Unsere Einrichtungen und Organisationen betreiben und nutzen heute viel mehr als nur „IT“, also Computer, Laptops, Smartphones. Bei genauerem Hinsehen fällt auf, dass im Laufe der Jahre viele weitere Systeme an die Netzwerke angeschlossen wurden.

Heute ist eine Vielzahl von Geräten und Anlagen mit unseren IT-Systemen vernetzt, die eine wichtige Rolle für Einrichtungen spielen und deren Funktionieren essenziell ist. Zum Beispiel:

- Lichtrufanlagen
- Telefonanlagen
- Elektronische Schließsysteme
- Heizungssteuerung
- Gebäudesteuerung
- Medizinprodukte
- Energiemanagement

Wer kümmert sich um diese Systeme? Sind Verantwortlichkeiten klar festgelegt? Können Gefahren oder Sicherheitsvorfälle von diesen Systemen ausgehen oder könnten diese Systeme Ziel von Cyberattacken werden?

Das vorliegende Dokument beschäftigt sich mit „Operational Technology“ in sozialen Einrichtungen und soll als Aufruf verstanden werden, einem bisher wenig beachteten Bereich mehr Aufmerksamkeit zu schenken.

2. Einordnung und Begrifflichkeiten

Eine klar definierte Grenze zwischen Informationstechnologie (IT) und operativer Technologie (OT) zu ziehen ist sehr schwierig. Daher soll zunächst versucht werden, die einzelnen Begriffe näher zu erläutern.

2.1. IT (Informationstechnologie)

Der Begriff Informationstechnologie (IT) ist der geläufigere der beiden und beschreibt strenggenommen die Gesamtheit aller Systeme und Anwendungen, die auf elektronischem Wege Daten verarbeiten, erstellen, speichern und/oder übertragen. Strenggenommen handelt es sich also um einen Überbegriff, der wiederum grob in die Teilgebiete Business-IT, Industrielle-IT, Kommunikations-IT und Unterhaltungs-IT unterteilt werden kann.

Für gewöhnlich wird dieser Begriff jedoch mit Computern, Notebooks, Servern, Smartphones, Tablets u. ä. assoziiert, auf denen Geschäftsanwendungen (Office-Pakete, Buchhaltungs-Anwendungen, Bewohnerverwaltungssysteme usw.) betrieben werden (also Business-IT).

2.2. OT (operative Technologie)

Für die Industrielle-IT hat sich mittlerweile der Fachbegriff „Operational Technology“ (Operative Technologie) oder kurz OT durchgesetzt. Hierunter versteht man die Gesamtheit der Hard- und Software, die physische Geräte, Prozesse und Ereignisse in einem Unternehmen überwacht und steuert. Die Bandbreite der Anwendungen und Systeme, die uns im Bereich der OT begegnen, ist groß. Hier eine (nicht vollständige) Aufzählung:

- Industrielle Steuerungssysteme (Industrial Control Systems, ICS)
- Speicherprogrammierbare Steuerungen (SPS oder Programmable Logic Controller, PLC). Hier als Überbegriff für eine SPS selbst, aber auch für Fernwirkgeräte (Remote Terminal Unit, RTU) und Programmable Automation Controller (PAC)
- Sensoren
- Aktoren, (Stellmotoren, CNC-Systeme usw.)
- Systeme und Anwendungen, die die oben genannten Komponenten überwachen und steuern (Supervisory Control and Data Acquisition, SCADA)

Am häufigsten dürften, im Kontext der Betrachtung, der Kontakt zu OT-Systemen in Form von technischen Gebäudeanlagen (z. B. Steuerungsanlagen für Heizungen, Blockheizkraftwerken u. ä. sowie Systeme für Beleuchtung, Beschattung und Klimatisierung) und medizinischen Geräten stattfinden. Wenn man den Kreis weiterzieht, dann könnten auch Videoüberwachungen, Alarmierungssysteme und somit dann auch TK-Anlagen in den Fokus genommen werden.

2.3. IoT (Internet of Things)

OT-Systeme werden schon seit langem untereinander vernetzt. Aufgrund gestiegener Anforderungen an Integration und Flexibilität erfolgt aber auch immer mehr eine Vernetzung mit Systemen und Anwendungen der Business-IT, bis hin zur Möglichkeit der Steuerung und Überwachung über Smartphones und von jedem Standort aus. Aus diesem Blickwinkel kann man dann vom „Internet of Things“ sprechen (IoT), da dieser Begriff ein Netzwerk physischer Objekte beschreibt, die mit Sensoren, Software und anderen Technologien Daten zwischen diesen Objekten austauschen.

3. Sicherheit im Umfeld von Operational Technology

In den letzten Jahren ist das Thema Sicherheit im Kontext Operational Technology immer weiter in den Fokus gerückt. Die erste bekannte (mutmaßlich von westlichen Staaten durchgeführte) Cyberattacke im Kontext OT erfolgt mit dem STUXNEX-Virus auf die Zentrifugen zur Uran-Anreicherung im Iran.

Das Marktforschungsunternehmen Gartner prognostiziert in den kommenden Jahren eine Zunahme an Cyberattacken mithilfe von OT[1].

Auf den folgenden Seiten werden wesentliche Herausforderungen aus dem besonderen Blickwinkel der Sozialwirtschaft näher beleuchtet.

3.1. Technische Herausforderungen

In der Vergangenheit war es üblich, Anwendungen und Systeme der OT physikalisch von denen der Business-IT zu trennen. Dies erfolgt heute aus Gründen der Integration, z. B. zur Vereinbarung von Wartungsarbeiten, nur noch selten bzw. wird ggf. nur noch bei stark erhöhten Schutzbedarfen umgesetzt. Auch kann es regulatorische Anforderungen geben, die eine Öffnung des OT-Netzwerkes (ggf. sogar über die Grenze der Einrichtung hinaus) erforderlich machen.

[1] Vgl. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

Ergänzend hierzu kommen in den OT-Netzen meist Netzwerkprotokolle zum Einsatz (z. B. Modbus, Profinet, Ethernet IP, Ethercat usw.), die einen primären Fokus auf Verfügbarkeit legen aber nicht auf Vertraulichkeit und/oder Integrität.
Unabhängig von der Tatsache, dass auch diese „Inselnetze“ sicher betrieben werden müssen, erhöht sich hierdurch die Angriffsoberfläche durch die Anbindung an andere Netze bzw. an das Internet.

Es bleibt festzustellen, dass verstärkt IT-Komponenten der Business-IT (commercial off-the-shelf, COTS) bei OT-Systemen zum Einsatz kommen und sich dadurch die Angriffsoberfläche weiter vergrößern kann. Auch kann es Vorgaben der Hersteller oder gesetzliche Anforderungen geben, die Veränderungen an Komponenten (Installation von Updates, Härtungsmaßnahmen) verhindern oder erschweren. Hierzu kann z. B. zählen, dass die Echtzeitfähigkeit des OT-Systems durch eine Härtungsmaßnahme ggf. eingeschränkt wird oder nicht mehr gegeben ist.

Echtzeitfähige Systeme müssen einerseits deterministisch sein und andererseits eine definierte Zykluszeit (die Zeit, die zwischen der Meldung des Sensors und die Weiterleitung des Signals an den Aktor vergehen darf) garantieren. In der Regel beträgt die garantierte Zykluszeit weniger als zehn Millisekunden.

Somit könnten die Herausforderungen an die IT-Sicherheit in den folgenden Punkten zusammengefasst werden:

- Lebenszyklus und Laufzeiten von OT-Lösungen sind deutlich höher als bei IT-Systemen, z. B. im Office-Umfeld. Wenn die Wartung herstellerseitig nicht mehr zur Verfügung steht, sind Updates oder Ersatzteile möglicherweise nicht mehr verfügbar.
- OT-Systeme sind möglicherweise gar nicht für das Einspielen von Aktualisierung/Verbesserungen vorbereitet.
- Systeme besitzen teilweise von Hause aus schon (schwerwiegende) Schwachstellen (kein „Security by Design“).
- Für die Kommunikation werden teilweise unsichere und/oder unverschlüsselte Protokolle verwendet.
- Systeme werden in einer unsicheren Grundkonfiguration (z. B. Standardpasswörter usw.) betrieben bzw. eine (unsichere) Grundkonfiguration lässt sich gar nicht anpassen.
- Grundlagen des sicheren Betriebs werden nicht angewendet (Benutzeranlage, Berechtigungsvergabe, Berechtigungskonzept, Datensicherung, Schutz vor Schadsoftware, Patchmanagement usw.)

Im BSI-Grundschutzkompendium finden sich eine Vielzahl von Bausteinen, mit denen sich OT-Systeme modellieren lassen. Mit den dort formulierten Anforderungen lässt sich die Angriffsoberfläche reduzieren, bis diese ggf. ein Niveau erreicht, bei dem eine Akzeptanz des Restrisikos durch die Unternehmensleitung möglich erscheint. Exemplarisch seien hier die Folgenden erwähnt:

- IND.1 Bauabteilungen
- IND.2.1 Allgemeine ICS-Komponente
- IND.2.2 Speicherprogrammierbare Steuerung (SPS)
- IND.2.3 Sensoren und Aktoren
- IND.3.2 Fernwartung im industriellen Umfeld

aber auch

- SYS.1.1 Allgemeiner Server (und Folgebausteine)
- SYS.2.1 Allgemeiner Client (und Folgebausteine)
- NET.1.1 Netzarchitektur und -design

Im Jahr 2021 hat Gartner die zehn wichtigsten High-Level-Maßnahmen veranschaulicht:

3.2. Organisatorische Herausforderungen

Ergänzend gibt es auch Schwierigkeiten organisatorischer Natur, die in den Planungs- und Beschaffungsprozessen für OT-Systeme begründet sein können. Beispielhaft wird hier dargestellt, wie der Prozess für die Inbetriebnahme von OT-Systemen (gilt ggf. auch für TK-Anlagen sowie für Alarmierungs- und Überwachungssysteme) in der Praxis oft abläuft:

1. Die Fachabteilung formuliert eine Anforderung und leitet diese an die Bauabteilung weiter.
2. Die Bauabteilung beauftragt einen Fachplaner.
3. Der Fachplaner evaluiert einen Realisierer für das Gewerk.
4. Umsetzung des Gewerkes durch den Realisierer.

Eine frühzeitige Einbindung der Unternehmens-IT, des Datenschutzbeauftragten (DSB) oder eines ggf. vorhandenen IT-Sicherheitsbeauftragten (ISB) erfolgt meist nicht. In vielen Fällen werden die genannten Organisationseinheiten erst zum Zeitpunkt der Inbetriebnahme oder auch erst nach der Fertigstellung eingebunden. Dies ist besonders für die Unternehmens-IT herausfordernd, da dann ad-hoc Maßnahmen für die Anbindung des OT-Systems in kurzer Zeit umgesetzt werden müssen.

Auch wird eine Korrektur an dieser Stelle schwierig, wenn seitens des DSB, des ISB oder der Unternehmens-IT festgestellt wird, dass das errichtete System ungeeignet ist bzw. grundlegende Anforderungen unterschreitet. Hier bleibt im Zweifelsfall nur noch eine dokumentierte Risikoakzeptanz durch die Unternehmensleitung, um den Weiterbetrieb zu ermöglichen.

Weitere Punkte, die organisatorische Herausforderungen darstellen könnten, sind:

- Unzureichende oder keine Möglichkeit der Bauabteilungen und der Fachplaner, die Themen IT-Betrieb, Datenschutz und IT-Sicherheit mit den hieraus resultierenden Verantwortungen und Anforderungen im Blick zu haben.
- Hinsichtlich der Themen IT-Betrieb, Datensicherheit und IT-Sicherheit fehlen den Fachplanern oft die Spezialisten, die die Auswirkungen abschätzen und den „Stand der Technik“ hinsichtlich der vorgenannten Themen berücksichtigen können.
- Man möchte die etablierten, vertrauensvollen Geschäftsbeziehungen zu einem Fachplaner nicht ändern.
- Bauabteilungen verlassen sich weitgehend auf die Entscheidungen der Fachplaner und können diese nicht in allen Spezialgebieten hinterfragen.
- Geringer Änderungswille bei allen Beteiligten, etablierte Prozesse zu ergänzen.

3.3. Umdenken erforderlich

In der Summe führen die technischen und organisatorischen Herausforderungen dazu, dass unsichere (oder sogar ungeeignete) Systeme in Betrieb genommen werden, dass Verantwortlichkeiten für Beschaffung und Betrieb nicht vollständig geklärt sind oder dass keine oder unvollständige Verträge für Wartung und Betrieb abgeschlossen wurden (in denen z. B. die Themen des sicheren IT-Betriebs nicht adressiert wurden).

Diese Form der Digitalisierung von Systemen und Geräten stellt Bauabteilungen und Fachplaner vor Herausforderungen. In ihren Abteilungen gibt es meist keine Experten für den IT-Betrieb, Datenschutz oder IT-Sicherheit. Diese arbeiten jedoch in vielen Unternehmen in der IT-Fachabteilung.

Durch kleine Änderungen in der Kommunikation zwischen den Beteiligten könnten bereits deutliche Verbesserungen in den Prozessen erzielt werden. Die frühzeitige Einbindung aller Stakeholder ist der Schlüssel zum Erfolg. So können alle Anforderungen im Projektmanagement berücksichtigt werden. Idealerweise wird diese in den entsprechenden Prozessen verankert.

Weiterhin ist es hilfreich, IT (und DSB und ggf. ISB) in die Rückmeldungsschleifen des Fachplaners an die Bauabteilung mit einzubeziehen. So können die Rückmeldungen durch Mitarbeitende mit entsprechendem Fachwissen ergänzend bewertet und ggf. erforderliche Korrekturmaßnahmen in die Wege geleitet werden.

Last but not least existieren ggf. schon etablierte Prozesse zur Prüfung von Anwendungen und Systemen durch DSB und ISB, sowie etablierte Konzepte für den sicheren IT-Betrieb (aus dem Bereich der Business-IT). Diese müssten dann lediglich auch bei der Beschaffung und dem Betrieb von OT-Systemen angewendet werden bzw. bedürfen nur kleinerer Adaptionen.

4. Risiken vermeiden – OT und IoT sicher im Betrieb

Auch in der Sozialwirtschaft lohnt es, vorhandene Strukturen und Zuständigkeiten im Kontext IT und OT auf den Prüfstand zu stellen. Die folgenden Maßnahmen sollen Orientierung für eine Verbesserung von Schutzmaßnahmen und der Ausfallsicherheit aufzeigen:

4.1. Was wir organisatorisch umsetzen – klare Zuständigkeiten

Eigentümer von Gebäuden	Gebäude-Eigentümer sind für den Betrieb verbauter OT-Systeme verantwortlich. Sie schließen die Verträge mit Dienstleistern. Über den Mietvertrag, der mit Gebäude-Nutzern geschlossen wird, sind Obliegenheiten bezüglich der OT-Systeme geregelt. Für alle OT-Systeme wird eine Datenbank (CMDB) mit den für den Betrieb zuständigen Betreibern geführt. Der Eigentümer koordiniert Anpassungen und Änderungen an OT-Systemen.
Geschäftsführung	Die Geschäftsführung etabliert einen Geschäftsprozess, in dem die Abläufe so aufeinander abgestimmt sind, dass bei Bauprojekten in der Planungs-, Umsetzungs- und Abschlussphase alle relevanten Stakeholder beteiligt werden. Die Geschäftsführung dokumentiert die Restrisikoübernahme für die geplanten OT-Anwendungen.
Bauabteilung / Projektmanagement	Im Rahmen des Projektmanagements wird bei der Planung des Gewerkes festgelegt, wer im Betrieb die operative Verantwortung für die OT-Systeme innehat. Für Ausschreibungen von OT-Systemen wird ein Kriterienkatalog auf Grundlage der Anforderungen aus den BSI-Bausteinen genutzt. Für geplante OT-Systeme werden in Zusammenarbeit mit dem künftigen Nutzer, dem Fachplaner, der IT-Abteilung, dem ISB und dem DSB Risikoanalysen erstellt.
IT-Abteilung	Die IT-Abteilung prüft alle geplanten OT-Systeme auf Kompatibilität zu den bestehenden IT-Systemen. Bekannte Probleme mit OT-Systemen werden an das Projektmanagement gemeldet.
Betreiber einer Einrichtung	Der Betreiber einer Einrichtung ist durch den Mietvertrag verpflichtet, die notwendige Sorgfalt bezüglich der genutzten OT-Systeme walten zu lassen. Bei Störungen der OT-Systeme ist er verpflichtet, unverzüglich den Eigentümer der OT-Systeme zu informieren.

4.2. Was wir technisch umsetzen – dokumentierte IT-Sicherheit

Risikoanalyse und Gefährdungsbeurteilung	Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat in seinem Kompendium OT-Bausteine definiert. In jedem Baustein werden die grundlegenden Gefährdungen und mögliche Maßnahmen zur Risikominimierung beschrieben. Diese Bausteine aus dem BSI-Kompendium können für eine Gefährdungsbeurteilung der geplanten Maßnahmen genutzt werden.
Sicherheitsvorgaben in Ausschreibungen	Im Rahmen der Projektplanung wird durch das Projektmanagement eine Risikoanalyse für die geplanten Gewerke und OT-Systeme durchgeführt. Durch die Erfüllung der in den BSI-Bausteinen beschriebenen IT-Sicherheitsanforderungen werden identifizierte OT-Risiken minimiert. Die Ergebnisse dieser Risikoanalyse werden für die Erstellung von IT-Sicherheitskriterien im Rahmen der Ausschreibung genutzt.
Konsequente Umsetzung – Sicherheit vor Kosten	Diese für die Ausschreibung erstellten Kriterienkataloge geben den Fachplanern konkrete Vorgaben für die Erfüllung der IT-Sicherheitsanforderungen vor. Eigentümer und Betreiber orientieren sich bei der Abnahme der Gewerke an den definierten IT-Sicherheitsanforderungen. Abweichungen müssen durch die Geschäftsführung dokumentiert und abgenommen werden.

5. Fazit

Der Umgang mit Operational Technology sollte als Teil von Digitalisierungsprozessen und der Strategieentwicklung in Sozialunternehmen geklärt werden. Mit der zunehmenden Vernetzung und der Vielzahl von Systemen und Geräten, die mit Netzwerk- und Internet-Anschluss ausgerüstet sind, spielt OT eine zentrale Rolle bei Gebäudemanagement, Energiemanagement und der Nutzung von Assistenzsystemen.

Zugleich müssen langfristige Folgen und die Auswirkungen in der IT-Sicherheitsstrategie bedacht werden. Denn operative Systeme spielen eine ebenso wichtige Rolle wie alle IT-bezogenen Komponenten bei der Gefahrenerkennung und -abwehr. IT und OT wachsen zusammen, nutzen teils gleiche Basistechnik und teilen Schnittstellen, so dass eine ganzheitliche Betrachtung unerlässlich ist.

Hier sind Einrichtungen und Träger in der Sozialwirtschaft gefragt, Rollen und Verantwortlichkeiten klar zu definieren:
Bei der Errichtung und Modernisierung von Gebäuden sollten relevante Akteure frühzeitig(er) eingebunden werden, um eine sichere und zuverlässige Nutzung von Geräten und Systemen im Rahmen der zunehmenden Vernetzung zu erreichen. Bei Einkauf und Montage von Systemen mit externen Schnittstellen sind die richtigen Ansprechpartner einzubinden.
Spätestens an dieser Stelle stellt sich die Frage, wer den Überblick über die verbaute Technik behält, für Wartung und Aktualisierung verantwortlich ist und zukünftig die technologische Entwicklung im Blick behält.

Veraltete und schlecht gewartete OT-Technik kann zu einem Sicherheitsrisiko für den gesamten IT-Betrieb führen. Das sollte bei der Auseinandersetzung mit dem Thema nicht außer Acht gelassen werden.

6. Glossar

Aktoren: Mechanische oder elektronische Vorrichtungen, die aufgrund von Signalen oder Befehlen physische Aktionen ausführen können. In industriellen Kontexten können Aktoren beispielsweise Stellmotoren oder CNC-Systeme sein.

BSI (Bundesamt für Sicherheit in der Informationstechnologie): Eine deutsche Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat mit Sitz in Bonn, die sich mit vertieften und hochspezialisierten Fragestellungen der IT-Sicherheit auseinandersetzt und einen maßgeblichen Beitrag zur Gewährleistung der Cyber-Sicherheit im nationalen und internationalen Kontext leistet.

CMDB (Configuration Management Database): Eine umfassende Datenbank, die zur systematischen Verwaltung von Informationen über die Konfiguration von IT-Systemen und -Geräten dient. Sie spielt eine Schlüsselrolle bei der Sicherstellung der Integrität und Verwaltbarkeit von IT-Infrastrukturen.

COTS (Commercial Off-The-Shelf): Standardisierte und kommerziell erhältliche Software- oder Hardwareprodukte, die nicht maßgeschneidert sind, sondern als vorgefertigte Lösungen auf dem Markt verfügbar sind. COTS-Produkte bieten oft Effizienz und Kostenvorteile, erfordern jedoch möglicherweise Anpassungen an die spezifischen Anforderungen.

Cyberattacken: Gezielte Angriffe auf Informationssysteme, bei denen potenzielle Angreifer versuchen, auf unerlaubte Weise auf Daten zuzugreifen, diese zu manipulieren oder anderweitig zu beeinträchtigen, oft mit dem Ziel, wertvolle Informationen oder Ressourcen zu erlangen oder Schaden zu verursachen.

DSB (Datenschutzbeauftragter): Eine Person, die in Unternehmen und Organisationen die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen hat und den Verantwortlichen bei der Umsetzung berät und unterstützt.

ICS-Komponente (Industrial Control System-Komponente): Eine essenzielle Komponente eines Industrial Control Systems (ICS), das in industriellen Umgebungen verwendet wird, um Prozesse, Anlagen und Systeme zu überwachen und zu steuern.

IoT (Internet of Things): Ein fortschrittliches Netzwerk physischer Objekte, die mit Sensoren, Software und Kommunikationstechnologien ausgestattet sind, um Informationen und Daten miteinander auszutauschen. Das IoT ermöglicht die Vernetzung und intelligente Steuerung einer breiten Palette von Geräten und Systemen.

ISB (Informationssicherheitsbeauftragter): Eine fachkundige und spezialisierte Person oder Einheit, die in Unternehmen und Organisationen für die Planung, Implementierung und Überwachung von IT-Sicherheitsmaßnahmen verantwortlich ist.

PAC (Programmable Automation Controller): Ein spezialisiertes Computersystem, das in industriellen Umgebungen eingesetzt wird, um Maschinen und Produktionsprozesse zu steuern. PACs kombinieren die Flexibilität von PCs mit der Robustheit von PLCs und bieten erweiterte Steuerungsfunktionen.

PLC (Programmable Logic Controller): Ein spezialisiertes Computersystem, das in industriellen Umgebungen eingesetzt wird, um Maschinen und Produktionsprozesse zu steuern. PLCs sind programmierbar und flexibel anpassbar, um den Anforderungen verschiedener Produktionsanlagen gerecht zu werden.

RTU (Remote Terminal Unit): Ein Gerät, das in der industriellen Automatisierung verwendet wird, um Daten aus Feldgeräten und Sensoren zu sammeln, zu verarbeiten und an übergeordnete Systeme, wie SCADA, weiterzuleiten.

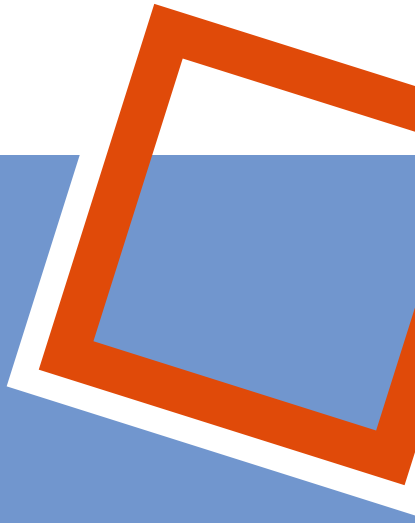
SCADA (Supervisory Control and Data Acquisition): Ein integriertes System zur Überwachung und Steuerung von industriellen Prozessen und Anlagen. SCADA-Systeme spielen eine entscheidende Rolle bei der Echtzeitüberwachung und -steuerung von Prozessen in industriellen Umgebungen.

Security by Design: Ein strategischer Ansatz zur Entwicklung von Informationssystemen, bei dem Sicherheitsaspekte von Anfang an in den Entwurfs- und Entwicklungsprozess integriert werden, um effektiven Schutz vor potenziellen Bedrohungen und Schwachstellen zu gewährleisten.

Sensoren: Messgeräte, die physikalische oder chemische Eigenschaften erfassen und in digitale Daten umwandeln. Sensoren sind unverzichtbar, um Echtzeitdaten in verschiedenen Anwendungsgebieten, einschließlich Industrieautomatisierung und Umweltüberwachung, zu generieren.

SPS (Speicherprogrammierbare Steuerungen): Hochspezialisierte Computer, die in der industriellen Automatisierung zur Steuerung und Überwachung von Maschinen und Anlagen eingesetzt werden. SPS-Systeme zeichnen sich durch ihre Robustheit und Zuverlässigkeit aus und spielen eine kritische Rolle in Produktionsprozessen.

STUXNET-Virus: Ein Computervirus, der 2010 entdeckt wurde und speziell auf die Sabotage von Industrieanlagen abzielte, insbesondere auf Kernkraftwerke und Wasserstoffanlagen. STUXNET gilt als eines der ersten bekannten Malware-Programme für Industriesteuerungssysteme (ICS).



Kontakt:

FINSOZ e.V.
Fachverband Informationstechnologie
in Sozialwirtschaft und Sozialverwaltung
Mandelstraße 16
10409 Berlin
Tel.: 030 42084-512
Fax: 030 42084-514
Mail: info@finsoz.de
www.finsoz.de

V.i.S.d.P: Michaela Grundmeier, Vorsitzende des Vorstandes

Ansprechpartner für den Lagebericht & Leitfaden:
FINSOZ-Fachgruppe „IT-Compliance“
Michaela Grundmeier
michaela.grundmeier@finsoz.de