Industrial Security Produkt Leitfaden

Systemübersicht mit bewährten Security-Praktiken

Weidmüller

Inhaltsübersicht

Warnung und Haftungsausschluss

Warnung
Geräte können unter unsicheren Betriebsbedingungen ausfallen und einen unkontrollierten Betrieb verursachen. Solche gefährlichen Ereignisse können zum Tod und/ oder zu schweren Verletzungen und/oder zu Sachschäden führen. Daher müssen Sicherheitseinrichtungen vorhanden sein wie elektrische Sicherheitskonzepte oder andere redundante Sicherheitseinrichtungen, die unabhängig vom Automatisierungssystem sind.

Haftungsausschluss
Dieser Leitfaden entbindet Sie nicht von der Verpflichtung zum sicheren Umgang bei Verwendung, Installation, Betrieb und Wartung. Jeder Anwender ist für den ordnungsgemäßen Betrieb seines Steuerungssystems selbst verantwortlich. Mit der Verwendung dieser Anleitung akzeptieren Sie, dass Weidmüller nicht für Sach- und / oder Personenschäden haftet, die durch die Verwendung entstehen können.

Hinweis
Die gegebenen Beschreibungen und Beispiele stellen keine kundenspezifischen Lösungen dar, sondern sind lediglich als Hilfe für typische Aufgabenstellungen gedacht. Für den ordnungsgemäßen Betrieb der beschriebenen Produkte ist der Anwender selbst verantwortlich. Dieser Leitfaden ist unverbindlich und erhebt keinen Anspruch auf Vollständigkeit in Bezug auf die Konfiguration sowie auf alle Eventualitäten. Mit der Nutzung dieses Leitfadens erkennen Sie an, dass wir für Schäden, die über den beschriebenen Haftungsrahmen hinausgehen, nicht haftbar gemacht werden können. Wir behalten uns das Recht vor, jederzeit und ohne Vorankündigung Änderungen an diesem Leitfaden vorzunehmen. Bei Widersprüchen zwischen den Vorschlägen des Leitfadens und anderen Weidmüller-Publikationen, wie z.B. Handbüchern, haben diese Inhalte stets Vorrang vor dem Leitfaden. Wir übernehmen keine Haftung für die in diesem Dokument enthaltenen Informationen.
Unsere Haftung, gleich aus welchem Rechtsgrund, für Schäden, die durch die Verwendung der in diesem Leitfaden beschriebenen Beispiele, Anleitungen, Programme, Projektierungs- und Leistungsdaten usw. entstehen, ist ausgeschlossen.

Sicherheitshinweise
Zum Schutz von Geräten, Systemen, Maschinen und Netzen vor Cyber-Bedrohungen ist es erforderlich, ein vollständiges, dem Stand der Technik entsprechendes industrielles Security-Konzept zu implementieren und zu pflegen. Der Kunde ist dafür verantwortlich, den unbefugten Zugang zu seinen Anlagen, Systemen, Maschinen und Netzen zu verhindern. Systeme, Maschinen und Komponenten sollten nur dann mit dem Unternehmensnetz oder dem Internet verbunden werden, wenn die notwendigen und angemessenen Sicherheitsvorkehrungen, wie Firewalls und Netzsegmentierung, getroffen wurden.

1. Einführung

Die rasche Digitalisierung und Vernetzung industrieller Prozesse hat die Betriebs- und Automatisierungstechnik (OT) verändert. Diese Fortschritte bieten zwar erhebliche Vorteile – wie höhere Effizienz, Flexibilität und Produktivität – bringen aber auch ernsthafte Herausforderungen mit sich, von denen die Cybersicherheit eine der dringendsten ist. Cyberangriffe auf industrielle Systeme werden immer häufiger, und ein erfolgreicher Angriff kann verheerende Folgen haben, darunter Produktionsausfälle, Umweltschäden oder sogar den Verlust von Menschenleben.

Da industrielle Systeme immer komplexer und vernetzter werden, reichen herkömmliche Sicherheitsmaßnahmen (Security-Maßnahmen) nicht mehr aus. Hacker und andere böswillige Akteure suchen aktiv nach Schwachstellen in OT-Netzwerken, um sie für Störungen oder Datendiebstahl auszunutzen. Es ist von entscheidender Bedeutung, dass Organisationen im OT-Sektor proaktive Schritte unternehmen, um ihre Systeme vor diesen Bedrohungen zu schützen.

Als Reaktion auf diese Herausforderungen haben die Regulierungsbehörden in der EU eine Reihe von Cybersicherheitsgesetzen und -richtlinien eingeführt, die neue Anforderungen an Unternehmen und Produkte stellen. Weidmüller unterstützt diese Initiativen mit einer Reihe von Lösungen, die die Sicherheit Ihrer Maschinen und Anlagen erhöhen.

Dieses Dokument bietet eine Anleitung zum Aufbau eines robusten Cybersicherheitssystems und zur Integration von Weidmüller Komponenten in dieses System. Dabei wird immer wieder auf die internationale Norm IEC 62443 verwiesen, die für die Cybersicherheitsanforderungen von industriellen Automatisierungssystemen entwickelt wurde. Diese Norm bietet einen umfassenden Rahmen für die Planung, Implementierung und Aufrechterhaltung von Sicherheitsmaßnahmen in OT-Netzwerken.
Weidmüller hat seinen sicheren Produktentwicklungsprozess nach IEC 62443-4-1 zertifiziert und wird auch nach IEC 62443-4-2 konforme Produkte einführen.

Zusätzlich zu dieser Übersicht sind auch detaillierte Security-Dokumente für bestimmte Produktgruppen verfügbar. Diese Dokumente bieten einen schnellen Zugriff auf Sicherheitsfunktionen, die für die Planung oder Durchführung von Sicherheitsrisikoanalysen genutzt werden können. Produktspezifische Sicherheitsdokumente finden Sie in unserem **eShop** oder im **Weidmüller Support Center**. Bitte suchen Sie nach Ihrem spezifischen Produkt.

www.weidmueller.de/eshop

www.weidmueller.com/support-center

Hinweis: Technische Informationen zum sicheren Einsatz und Betrieb unserer Produkte finden Sie im Kapitel "Defense-in-Depth".

1.1 Unterschied zwischen IT und OT

Informationstechnologie (IT) und Betriebstechnologie (OT) sind zwei Schlüsselbereiche in Industrieunternehmen. Obwohl sie oft miteinander verbunden sind und sich gegenseitig ergänzen, dienen sie unterschiedlichen Zwecken und stehen vor unterschiedlichen Herausforderungen.

IT (Informationstechnologie) befasst sich mit der Verarbeitung, Speicherung und Übertragung von Daten. Sie unterstützt Geschäftsprozesse und Verwaltungsaufgaben durch Systeme wie Computernetzwerke, Datenbanken und Softwareanwendungen. In der IT konzentriert sich die Security in erster Linie auf den Schutz von Daten vor unberechtigtem Zugriff, Diebstahl oder Manipulation. Die Prioritäten in der IT-Security sind:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

OT (Operational Technology) umfasst die Steuerung, Überwachung und Automatisierung von physikalischen Prozessen und Maschinen in industriellen Umgebungen. Dazu gehören Geräte wie Sensoren, Aktoren, industrielle Steuerungssysteme und Roboter. In der OT liegt der Schwerpunkt auf der Gewährleistung des kontinuierlichen Betriebs und der Security von Systemen und Infrastrukturen. OT-Umgebungen erfordern spezielle Security-Lösungen, die über die in der IT verwendeten Lösungen hinausgehen.

Die Security-Prioritäten in der OT sind:

Abbildung 1 : Priorität der OT-Security

1.2 Der Unterschied zwischen Security und Safety

Security bezieht sich auf den Schutz digitaler oder physischer Güter vor böswilligen Handlungen oder unbefugtem Zugriff. Dazu gehört der Schutz von Computern, Netzwerken, Software und Daten vor Cyberangriffen, Hackerangriffen, Malware und anderen Bedrohungen. In OT-Umgebungen erstreckt sich die Sicherheit auch auf den Schutz von Industrieanlagen, Produktionsprozessen und kritischer Infrastruktur vor Schäden, Sabotage, Ausfällen und Cyberangriffen.

Im Gegensatz dazu konzentriert sich **Safety** auf den Schutz von Menschen, der Umwelt und der materiellen Ressourcen vor Gefahren und Unfällen. Safety zielt darauf ab, das körperliche Wohlbefinden der Mitarbeiter zu gewährleisten, Verletzungen zu verhindern und industrielle Katastrophen oder Umweltschäden zu vermeiden.

Beide, Security und Safety, sind für die Gewährleistung der allgemeinen Integrität und Zuverlässigkeit von Systemen unerlässlich. Das Erreichen von Safety ist unmöglich, wenn nicht auch die Security berücksichtigt wird.

2. Security-Gesetze und -standards

Bis vor kurzem konzentrierten sich die Security-Gesetze vor allem auf kritische Infrastrukturen. Aufgrund der zunehmenden Bedrohung durch Cyberangriffe werden durch neue Vorschriften die Anforderungen an die Cybersicherheit für Unternehmen und Produkte in verschiedenen Branchen erweitert.

Gesetz	Region	Zielgruppe	Kommentare
NIS (Network Information System Security) EU 2016/1148	EU	Eigentümer von Vermögenswerten, Betreiber von kritischen Infrastrukturen	Verlangt die Einführung eines Cybersicherheitsmanagementsystems. Wird durch nationale Gesetze in den EU-Ländern durchgesetzt.
Cybersecurity and Infrastructure Security Agency Act	USA	Asset Owner, Betreiber von kritischen Infrastrukturen	Verlangt die Einführung eines Cybersicherheitsmanagementsystems für kritische Infrastrukturen.w

2.1 Neue und erweiterte Sicherheitsgesetze

Da Cyber-Bedrohungen ein zunehmendes wirtschaftliches Risiko darstellen, werden die Sicherheitsanforderungen für Unternehmen und Produkte erheblich ausgeweitet. Vor allem die EU führt neue oder erweiterte Gesetze mit Bestimmungen zur Cybersicherheit ein.

Recht	Obligatorisch von	Zielgruppe	Kommentare
NIS2 (Network Information System Security) EU 2022/2555	EU-Ziel: Okt. 2024	Anlagenbetreiber	Ausweitung des Anwendungsbereichs der NIS auf weitere Industriezweige (z. B. Maschinenbau, Elektroindustrie) und kleinere Unternehmen (>50 Beschäftigte, >10 Mio. € Umsatz). Umsetzung in nationales Recht notwendig.
RED DA (Cyber Resilience Act) EU 2033/30	Aug. 2025	Geräte-/Maschinenhersteller	CE-Kennzeichnungspflicht für Geräte mit Funk-Schnittstellen, die direkt oder indirekt mit dem Internet kommunizieren können.
Maschinenverordnung EU 2023/1230	Jan. 2027	Hersteller von Maschinen	CE-Kennzeichnungspflicht für Maschinen. Neue Sicherheitsanforderungen.
CRA (Cyber Resilience Act) EU 2024/2847	Dez. 2027	Geräte-/Maschinenhersteller	CE-Kennzeichnungspflicht für Geräte oder Software mit digitalen Elementen und Datenkommunikation.

2.2 Branchenspezifische Sicherheitsstandards

Einige Organisationen haben für bestimmte Wirtschaftszweige Cybersicherheitsanforderungen eingeführt.

Normen von Organisationen	Obligatorisch von	Zielgruppe	Kommentare
IACS UR-E26/27	Juli 2024	Schiffseigner, Schiffsbetreiber.	Normen der International Association of Classification Societies (IACS), die Cybersicherheitssysteme für neue Schiffe vorschreiben.

2.3 Internationale Security-Standards

Cybersicherheit geht über die Sicherung einzelner Komponenten hinaus; sie erfordert einen ganzheitlichen Ansatz zum Schutz von Systemen, Netzwerken, Daten und Infrastrukturen auf mehreren Ebenen. Es muss ein umfassendes Security-Managementsystem (CSMS) vorhanden sein, dass die Anforderungen für die Einrichtung, Umsetzung, Pflege und kontinuierliche Verbesserung von Cybersicherheitsmaßnahmen definiert. Nachstehend finden Sie die wichtigsten internationalen Normen, die für die Cybersicherheit relevant sind.

Standard	Schwerpunkt	Zielgruppe	Kommentare
ISO / IEC 27001	IT	Anlageneigentümer, Anlagenbetreiber	Definiert ein Informationssicherheitsmanagementsystem (ISMS) mit Schwerpunkt auf der IT-Sicherheit
ISA / IEC 62443	OT + IT	Anlageneigentümer, Anlagenbetreiber, Hersteller des Geräts	Definiert ein Cybersecurity Management System (CSMS) für OT und IT, das Anforderungen an Betreiber, Systemintegratoren und Komponentenhersteller enthält.

2.3.1 Norm IEC 62443

Die Normfamilie IEC 62443 beinhaltet eine Reihe von internationalen Normen und technischen Berichten, die speziell für die Cybersicherheit von industriellen Automatisierungssystemen entwickelt wurden. Die Norm wurde von der Internationalen Elektrotechnischen Kommission (IEC) entwickelt, um den spezifischen Anforderungen und Herausforderungen von OT-Systemen gerecht zu werden und klare Richtlinien für die Implementierung von Sicherheitskontrollen und -verfahren in industriellen Umgebungen bereitzustellen.

Die Norm deckt die folgenden Aspekte ab:

- Sicherheit im Netz
- Sicherheitsrichtlinien und -verfahren
- Risikomanagement
- Cybersichere Entwicklung und Wartung von Systemen
- Security-Bewertung und -zertifizierung

Jeder Teil ist so konzipiert, dass er sich an verschiedene Interessengruppen wie Anlagenbetreiber, Systemintegratoren und Komponentenhersteller richtet. Zum Beispiel bietet IEC 62443-2-1 eine Zuordnung zu ISO 27001, die sich auf IT-Security konzentriert und einen umfassenden Ansatz für OT-Security ermöglicht. Die IEC 62443 kann daher umfassend für die OT-Security genutzt werden.

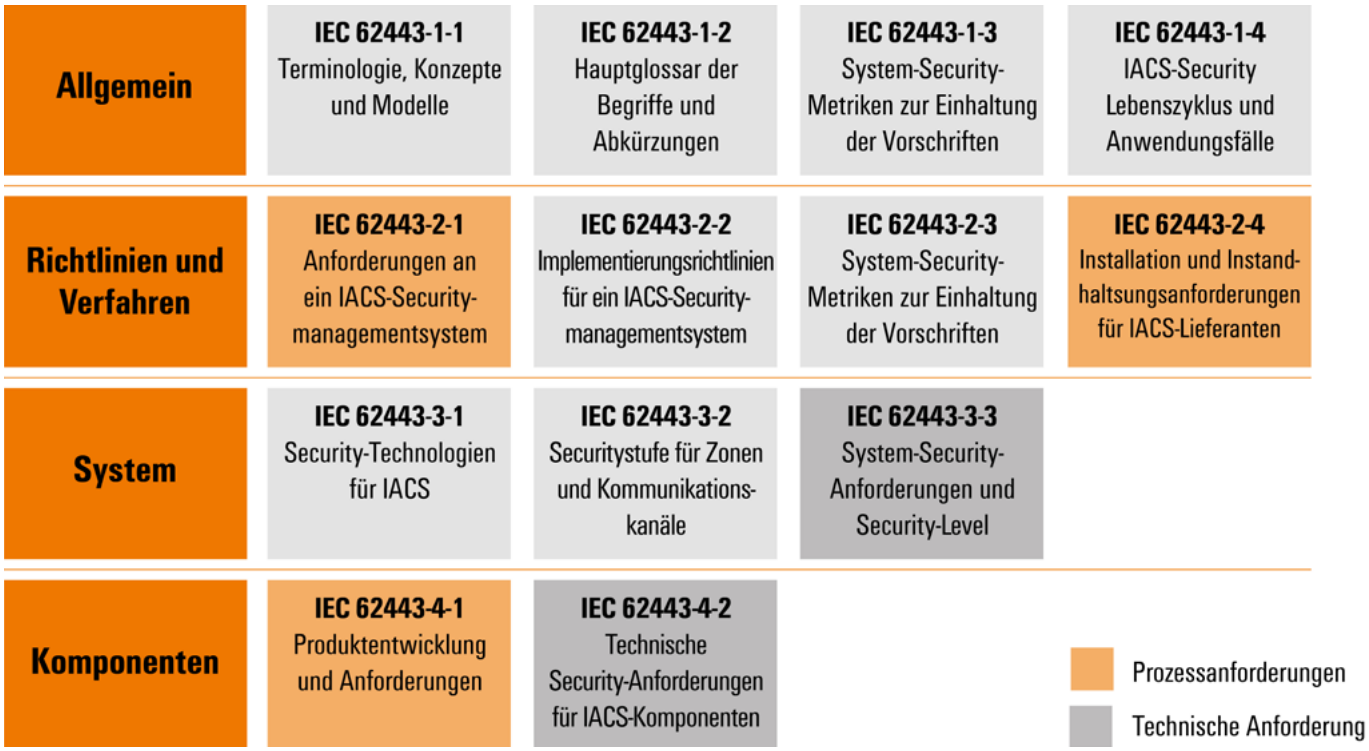

Abbildung 2 : Teile der IEC 62443

Das Cyber Security Management System (CSMS) der IEC 62443 basiert auf den folgenden Kernelementen:

Wirtschaftlichkeit
Die geschäftliche Begründung soll klären, welche Geschäftselemente geschützt werden sollen und wie wichtig sie für das Unternehmen im Falle eines erfolgreichen Cyberangriffs sind. Dazu gehören finanzielle Aspekte ebenso wie Sicherheits-, Gesundheits-, Umwelt- und Reputationsaspekte

Identifizierung, Klassifizierung und Bewertung von Risiken
Identifizierung der Cyberrisiken, mit denen eine Organisation konfrontiert ist, und Bewertung der Wahrscheinlichkeit und Schwere dieser Risiken.

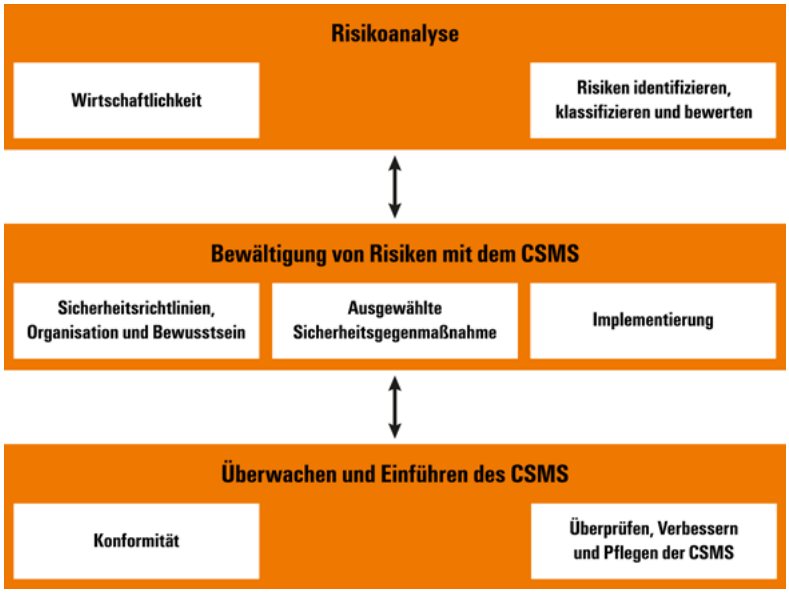

Abbildung 3 : Cyber Security Management System (CSMS)

Sicherheitsrichtlinien, Organisation und Bewusstsein
Dieser Teil behandelt strategische und organisatorische Themen wie:

- Umfang des Security-Managementsystems
- Organisation für Secrurity
- Mitarbeiterschulung und Sicherheitsbewusstsein
- Plan zur Aufrechterhaltung des Geschäftsbetriebs
- Security-Richtlinien und -Verfahren

Ausgewählte Security-Gegenmaßnahmen
Festlegung von Securitykontrollen mindestens für die wichtigsten Elemente:

- Persönliche Security
- Physische und ökologische Security
- Segmentierung des Netzes
- Zugangskontrolle

Umsetzung: Umsetzung von Maßnahmen zur Risikominderung und zum Erreichen von Sicherheitszielen.

Konformität: Sicherstellen, dass das für eine Organisation entwickelte CSMS eingehalten wird.

Überprüfung, Verbesserung und Pflege des CSMS: Sicherstellen, dass das CSMS im Laufe der Zeit weiterhin seine Ziele erreicht.

Weidmüller Compliance

Weidmüller hat einen zertifizierten sicheren Produktentwicklungsprozess nach IEC 62443-4-1 implementiert und bietet sichere Produkte nach IEC 62443-4-2 an

2.4 Nordamerikanische Cybersicherheitsrichtlinien für OT-Umgebungen

2.4.1 Cyber Resilience Act (CRA)

Obwohl die CRA in erster Linie eine EU-Initiative ist, müssen auch nordamerikanische Organisationen ihre Auswirkungen berücksichtigen, insbesondere wenn sie Produkte für europäische Märkte herstellen oder liefern. Die CRA konzentriert sich auf die Gewährleistung der **Cybersicherheit digitaler Produkte** während ihres gesamten Lebenszyklus, einschließlich der sicheren Entwicklung, Bereitstellung und Wartung.

2.4.2 Hauptaspekte für Nordamerika

- **Produktkonformität:** Die Hersteller müssen sicherstellen, dass ihre OT-Systeme entsprechend „Secure-by-Design" konzipiert sind und sichere Updates unterstützen.
- **Digitale Elemente:** Alle OT-Produkte oder -Software mit digitalen Kommunikationselementen (z. B. industrielle IoT-Geräte) sollten die in der CRA dargelegten Security-Standards erfüllen.

2.4.2.1 Schlüsselebenen für nordamerikanische Organisationen:

- **Cybersicherheitsmanagementsystem (CSMS):** Einführung eines strukturierten Cybersicherheitsmanagementprozesses.
- **Netzsegmentierung:** Verwenden Sie Zonen und Conduits, um Sicherheitsrisiken zu begrenzen (z. B. sichere Zonen für kritische Prozesse).
- **Gerätesicherheit:** Die Hersteller müssen bei Geräten und Komponenten, die in OT-Umgebungen eingesetzt werden, die Grundsätze des "Secure-by-Design" beachten.

2.4.3 ISA/IEC 62443 für OT-Sicherheit

ISA/IEC 62443 ist eine umfassende Norm für Cybersicherheit in industriellen Automatisierungs- und Steuerungssystemen. Sie bietet einen Rahmen für die Sicherung von OT-Umgebungen, vom Anlagenbetreiber bis zum Komponentenhersteller.

2.4.4 NIST-Normen (NIST 2.0)

Das **National Institute of Standards and Technology (NIST)** bietet einen Rahmen für Cybersicherheit, der in vielen nordamerikanischen Branchen, einschließlich kritischer Infrastrukturen und OT-Umgebungen, eingesetzt wird. Die neueste Version, NIST 2.0, konzentriert sich auf proaktive Sicherheitsmaßnahmen und die Verbesserung der Widerstandsfähigkeit gegenüber Cyberangriffen.

2.4.4.1 NIST 2.0 Schlüsselelemente für OT:

- **Identifizieren:** Verstehen und katalogisieren Sie OT-Assets und Risiken.
- **Schützen Sie sich:** Implementieren Sie Sicherheitsvorkehrungen wie Firewalls, VPNs und sichere Authentifizierung.
- **Erkennen:** Überwachen Sie OT-Umgebungen mithilfe von Intrusion Detection Systemen (IDS) auf potenzielle Bedrohungen.
- **Reagieren:** Erstellen Sie auf OT-spezifische Szenarien zugeschnittene Reaktionspläne für Vorfälle.
- **Wiederherstellen:** Stellen Sie sicher, dass Pläne für die Notfallwiederherstellung und Geschäftskontinuität vorhanden sind.

2.4.4.2 Vergleichende Tabelle

Standard	Schwerpunkt	Anwendbare Bereiche
CRA	Security im digitalen Produktlebenszyklus	Hersteller von OT-Geräten und Software
ISA / IEC 62443	Cybersecurity für OT-Umgebungen	Anlagenbesitzer, Integratoren und Komponentenhersteller
NST 2.0	Umfassender Rahmen für die Cybersicherheit	Anlagenbesitzer und Anbieter kritischer Infrastrukturen

3. Defense-in-Depth

Das Sicherheitskonzept "Defense-in-depth" ist ein strategischer Ansatz, der darauf abzielt, Systeme und Netze durch die Implementierung mehrerer Sicherheitsschichten vor einer Vielzahl von Bedrohungen zu schützen. Die Idee hinter diesem Konzept ist, dass eine einzige Sicherheitsmaßnahme nicht ausreicht, um ein System vollständig zu schützen. Stattdessen werden mehrere Sicherheitsebenen oder -schichten implementiert, um potenzielle Angriffe auf verschiedenen Ebenen zu erkennen, zu verhindern oder zu entschärfen.
Defense-in-depth ist eine vielschichtige Strategie, die Menschen, Technologie und operative Fähigkeiten integriert, um variable Barrieren über mehrere Ebenen und Dimensionen der Organisation hinweg zu errichten.

Es gibt verschiedene Ebenen:

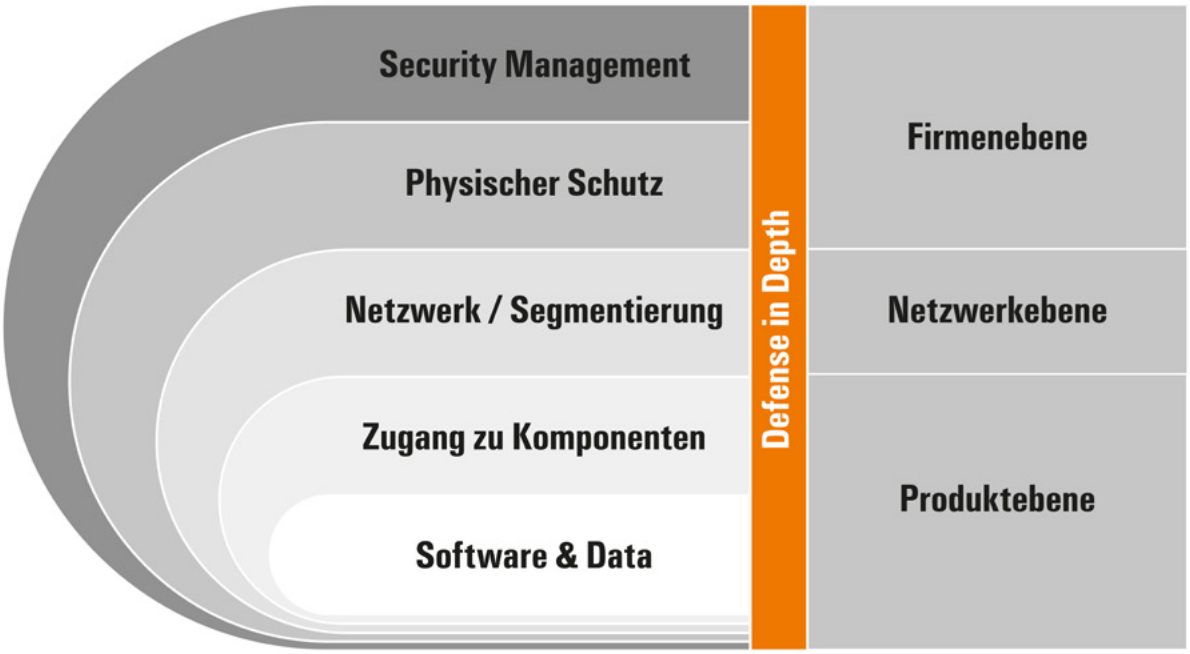

Abbildung 4 : Schichtenmodell "Defense-in-depth"

Die folgenden Abschnitte beschreiben die einzelnen Ebenen und wie Weidmüller Komponenten Sie beim Aufbau eines Sicherheitssystems unterstützen können.

3.1 Defense-in-Depth Schicht: Security Management

Das „Security Management“ ist ein übergeordnetes Cybersicherheitsprogramm, das den Sicherheitsschutz der OT-Umgebung unterstützt. Diese Ebene bezieht sich speziell auf organisatorische Themen, indem sie ein Cybersicherheitsmanagementsystem einrichtet (siehe obiges Kapitel "Norm IEC 62443" als Beispiel). Dazu gehören Richtlinien, Prozesse und Bewusstseinsschärfung. Diese Regularien und Prozesse werden die anderen Schichten von „Defense in Dept“ bzgl. erforderlichen Entscheidungen leiten und beeinflussen.

Typische Themen in dieser Ebene sind:

- Sensibilisierung und Schulung des Personals
- Definition/Überprüfung der Verantwortlichkeiten der Anlagennutzer
- Definition/Überprüfung von Benutzerrollen
- Definition/Überprüfung von Benutzerzugriffsrechten
- Regelung des physischen Zugangs
- Umsetzung eines Reaktionsplans nach einem Security-Vorfall
- Definition eines Patch-Management-Systems für die Verteilung von Sicherheits-Patches

3.1.1 PSIRT

PSIRT steht für "Product Security Incident Response Team". Das PSIRT ist ein spezialisiertes Team innerhalb eines Unternehmens oder einer Organisation, dass sich mit der Behebung von Security-Vorfällen in Produkten oder Software befasst. Wenn Sicherheitslücken oder Schwachstellen in einem Produkt entdeckt werden, ist das PSIRT für deren Untersuchung, Bewertung und Behebung zuständig. Darüber hinaus kommuniziert ein PSIRT mit Kunden, Lieferanten und anderen relevanten Parteien, um Informationen über Sicherheitsprobleme zu verbreiten und Lösungen anzubieten.
Weidmüller hat ein PSIRT eingerichtet und informiert auf der Weidmüller-Website **"Security Adivsory Board"** über produktspezifische Sicherheitsschwachstellen und deren Behebung.

www.weidmueller.com/security-advisory-board

Darüber hinaus veröffentlicht Weidmüller Sicherheitslücken seiner Produkte bei **CERT@VDE**. CERT@VDE ist eine neutrale, nicht gewinnorientierte Plattform. Das CERT@VDE unterstützt seine Partner in Fragen der Cybersecurity in Produkten der Automatisierungsbranche, um eine schnelle, strukturierte und professionelle Bearbeitung von Sicherheitslücken zu ermöglichen.

www.cert.vde.com

3.1.2 CSIRT

CSIRT steht für "Computer Security Incident Response Team". Im Gegensatz zu einem PSIRT konzentriert sich ein CSIRT nicht nur auf Produkte, sondern auch auf die allgemeine IT-Infrastruktur einer Organisation. Ein CSIRT ist für die Erkennung, Behebung und Verwaltung von Sicherheitsvorfällen in einem breiteren Kontext zuständig.

3.2 Defense-in-Depth Schicht: Physischer Schutz

Physische Sicherheitsmaßnahmen sollen das Risiko eines zufälligen oder vorsätzlichen Verlusts oder einer Beschädigung von Vermögenswerten und der Umgebung verringern

Examples of a physical access control

- Generell sollte der Personenkreis, der eine Zugangsberechtigung hat, möglichst klein gehalten werden.
- Sichern Sie Ihre Schranktüren mit einem verbesserten Zugriffsschutz, z.B. mit Schlüsseln.
- Sichere, von außen zugängliche Serviceschnittstellen, zum Beispiel mit dem abschließbaren System FrontCom Vario von Weidmüller.

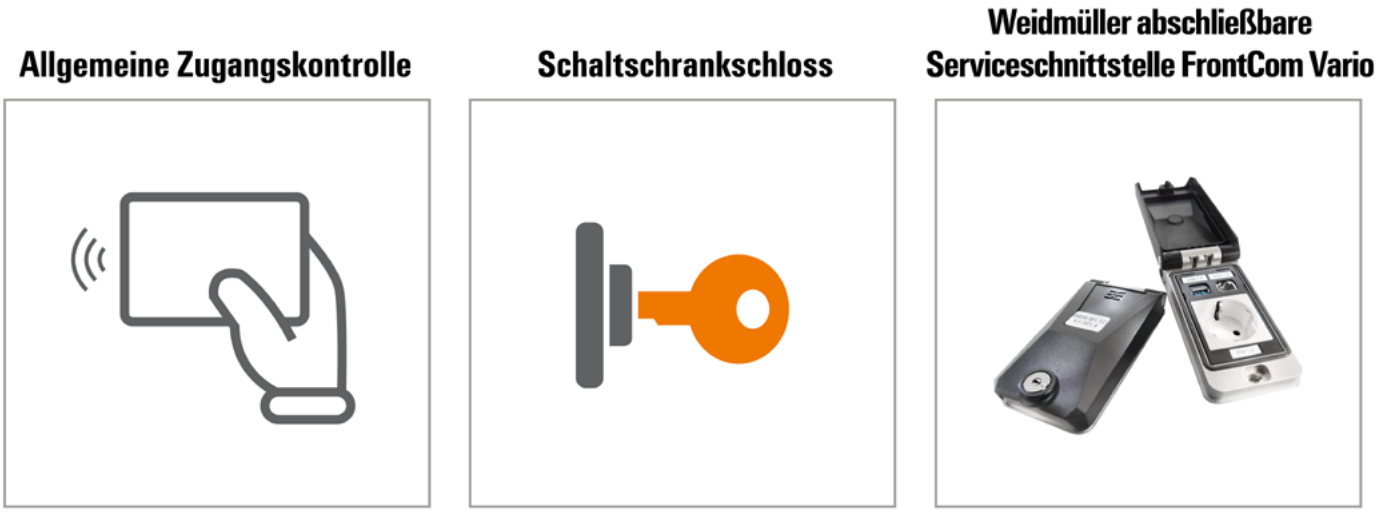

Abbildung 5 : Beispiele für physische Zugangssysteme

Anmerkung:
Die Weidmüller Komponenten sind für den Einsatz in industrieller Umgebung vorgesehen. Weidmüller IP20-Komponenten sind für den Betrieb in einem geschützten Gehäuse konzipiert. Der physische Zugang zu den Geräten sollte nur autorisierten Personen gestattet werden

3.3 Defense-in-Depth Schicht: Netzwerk / Segmentierung

Das Netzwerk ist ein Hauptziel für Cyberangriffe. Eine wesentliche Gegenmaßnahme ist die Segmentierung des Netzes, um einen möglichen Angriff auf einen begrenzten Bereich zu beschränken.

Grundprinzipien der Netzsegmentierung (Zonen und Conduits)

a. Vermeiden Sie große Zonen: Große Zonen können Schwachstellen schaffen. Wenn Sie die Zonen klein halten, können Sie potenzielle Bedrohungen eindämmen.
b. Definieren Sie hierarchische Zonen: Richten Sie Zonen auf demselben Security-Niveau ein, um die Verwaltung zu vereinfachen und die Sicherheit zu erhöhen.
c. Sichere Übergänge (Conduits): Stellen Sie sicher, dass die Übergänge zwischen den Zonen gut geschützt sind. Verwenden Sie Firewalls, um die Kommunikation auf das Notwendigste zu beschränken.

Als Beispiel wird hier eine Netzarchitektur mit Zonen und Conduits gezeigt.

Zone: gelbes Segment. Eine Gruppe von Komponenten mit demselben Zielniveau.

Conduit: orangefarbene Linie. Geschützter" Kanal für den Datenaustausch.

Normalerweise schützt ein Router mit seiner Firewall ein Conduit damit nur die notwendige Kommunikation zugelassen wird. Die Kommunikation in einem Conduit sollte nach Möglichkeit verschlüsselt sein. Wenn das verwendete Protokoll dies nicht vorsieht, sollte ein sicherer Kanal (über VPN-Tunnel) oder eine sichere verschlüsselte Kommunikation, z. B. HTTPS, OPC-UA verwendet werden.

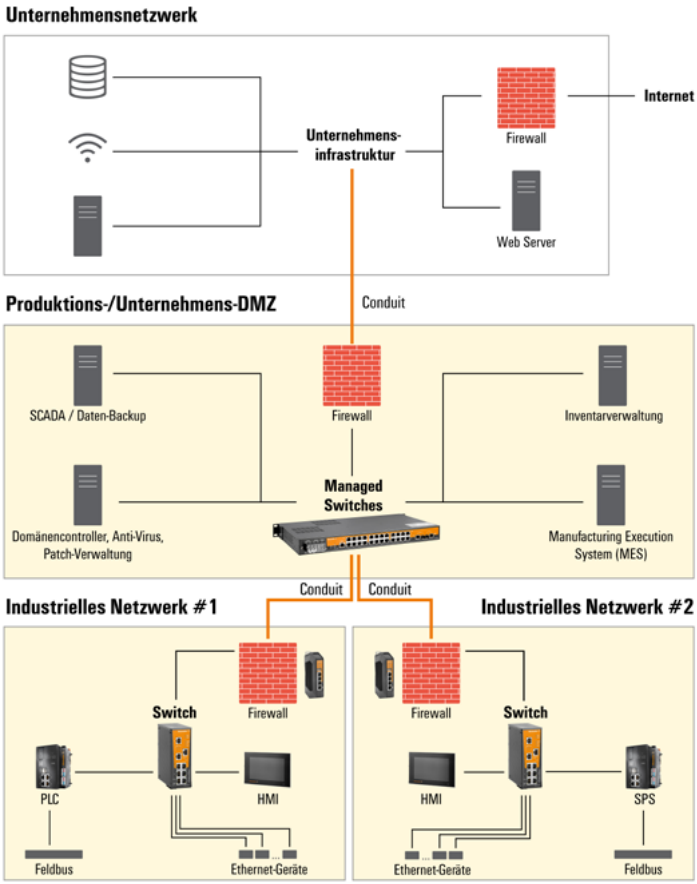

Abbildung 6 : Konzept Zonen und Leitungen

Es gibt verschiedene Systemkonzepte für Zonen und Leitungen, wie in der Abbildung dargestellt. Ein Unternehmen muss individuell über die optimale Architektur entscheiden, obwohl die Grundprinzipien identisch sind.

Die DMZ steht für „Demilitarized" Zone und bezeichnet ein speziell kontrolliertes Netz, das sich zwischen dem externen Netz (Internet) und dem internen Netz oder zwischen zwei kritischen internen Netzen befindet. Es handelt sich um eine Art Pufferzone, die die Netze durch strenge Kommunikationsregeln und Firewalls voneinander trennt.

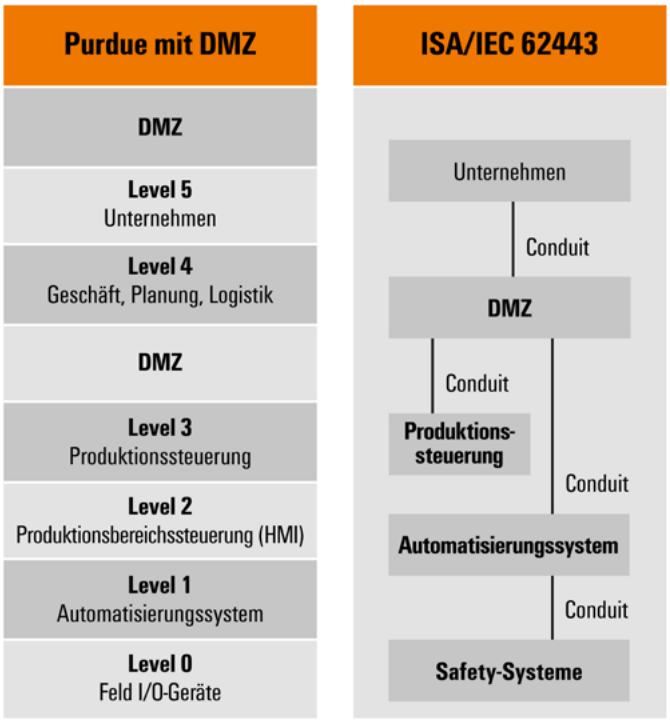

Abbildung 7 : Verschiedene Zonenkonzepte

Nachfolgend ein Beispiel für die Automatisierungsstruktur einer Maschine und die OT-Netzwerkinfrastruktur der Fabrikhalle mit Weidmüller-Komponenten.

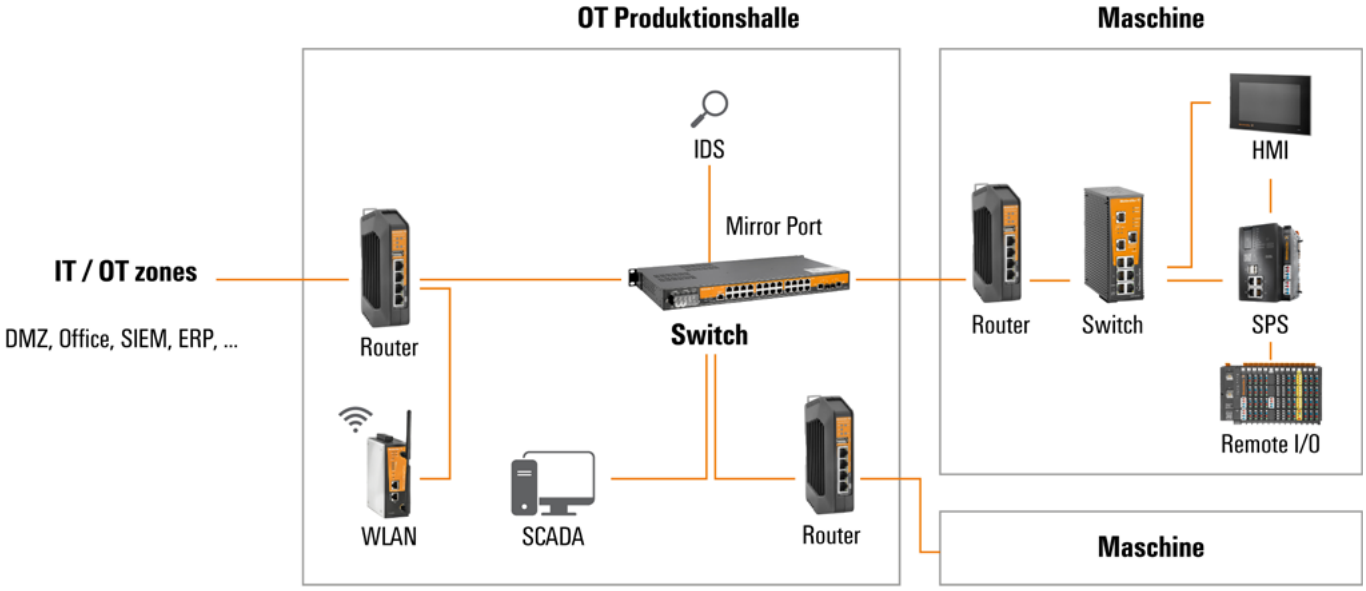

Abbildung 8 : Beispiel für eine Netzsegmentierungsstruktur.

Bewährte Security-Praktiken für Netzwerksegmentierung

- **Netzwerke segmentieren:** Segmentieren Sie das Netz in Zonen mit dem gleichen Security-Niveau. Erstellen Sie Zonen innerhalb von Maschinen und der OT-Fläche mit Routern, VLANs oder Layer-3-Switches.
- **Verwenden Sie Firewalls:** Sichern Sie Ihre Rechner mit Routern, die mit Firewalls ausgestattet sind, entweder integriert oder extern positioniert.
- **Schützen Sie Feldbusnetzwerke:** Implementieren Sie physische Zugangskontrollen für Feldbussegmente aufgrund ihres geringen Security-Niveaus.
- **Isolieren Sie Wi-Fi-Netzwerke:** Verwenden Sie separate VLANs für den Wi-Fi-Zugang, begleitet von robusten Sicherheitsmaßnahmen wie Firewall-Regeln und zentraler Zugangsverwaltung (z. B. IEEE 802.1X).
- **Erwägen Sie Intrusion Detection Systems (IDS):** Setzen Sie IDS zur Überwachung von Angriffen ein und nutzen Sie Mirror-Ports von Managed Switch zur Analyse des Datenverkehrs.

Die folgenden Konzepte unterstützen die Sicherheit der Netzwerksegmentierung.

3.3.1 Switche und VLAN

Ein VLAN (Virtual Local Area Network) ist ein logisches Netz, das innerhalb eines physischen Netzes eingerichtet wird. Es ermöglicht die Segmentierung und Organisation von Geräten in Netzwerken unabhängig von ihrer physischen Position.

Traditionell werden die Geräte in einem Netzwerk durch physische Verbindungen segmentiert. VLANs hingegen ermöglichen es, Geräte in einem Netzwerk nach logischen Kriterien wie Funktion, Abteilung, Anwendung oder Security-Niveau zu gruppieren, unabhängig von ihrer physischen Position im Netzwerk. Diese Segmentierung bietet mehr Flexibilität, Sicherheit und eine effizientere Nutzung von Ressourcen.

Die Managed Switches von Weidmüller bieten portbasierte VLAN- (Virtual Local Area Network) und Tagged-VLAN-Unterstützung und ermöglichen so eine logische Segmentierung des Netzwerks. So lassen sich einfach Netzwerksegmente mit unterschiedlichen Sicherheitsstufen in der Maschine, in der Produktionslinie oder in der Anlage einrichten.

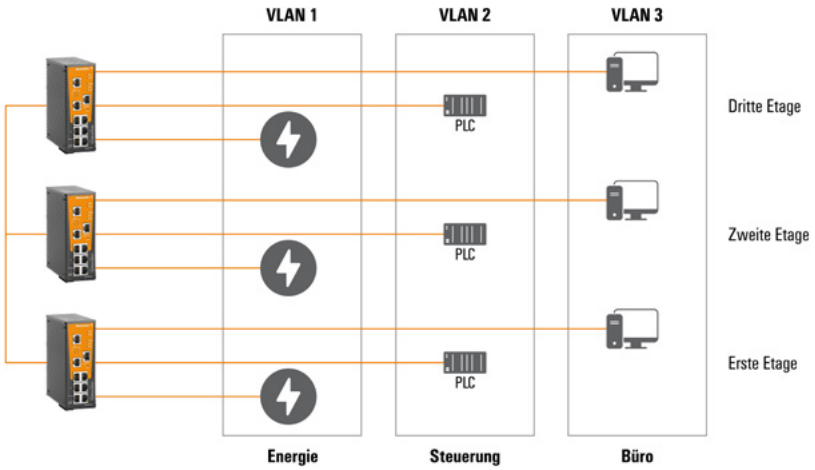

Abbildung 9 : VLAN-Segmentierung

Ein typisches Beispiel für ein VLAN ist die logische Trennung eines Energieerfassungsnetzwerkes (z.B. Weidmüller Energy Meter mit Modbus TCP) von einem produktionsrelevanten Netzwerk. Beide Netzwerke nutzen das gleiche physikalische Netzwerk und es muss keine zusätzliche Verkabelung vorgenommen werden.

Sie können Weidmüller Ethernet-Switches auch in Verbindung mit Feldbussystemen wie PROFINET oder EtherNet/IP einsetzen. Bitte beachten Sie die technischen Daten der Switches.

Weitere Informationen zur Sicherheit am Feldbus finden Sie im Kapitel " 3.3.3 Feldbus ".

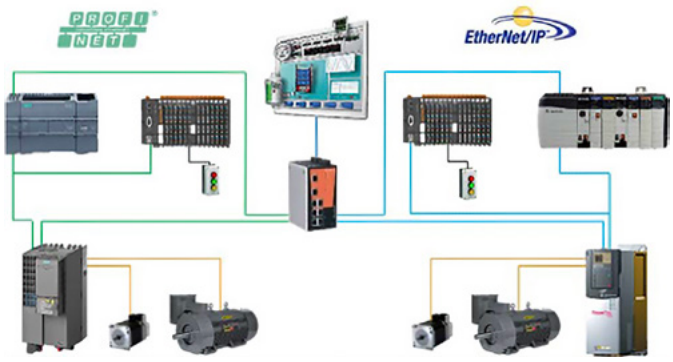

Abbildung 10 : Feldbusnetzwerk mit Switch

Bewährte Security-Praktiken für Switche und VLAN's

- **Implementieren Sie VLANs:** Verwenden Sie VLANs, um Netzwerke nach Sicherheitskritikalität zu segmentieren (z. B. getrennte Wi-Fi-Zugangspunkte oder Energiezähler).
- **Sichere Benutzerschnittstellen:** Deaktivieren Sie HTTP und verwenden Sie HTTPS für Webschnittstellen. Deaktivieren Sie TELNET zu Gunsten von SSH für den CLI-Zugang. Setzen Sie optional die Management-VLAN-ID des Switches auf ein separates VLAN, damit die Webschnittstelle des Switches nur über ein separates VLAN erreicht werden kann (z. B. nur ein Port im Netzwerksystem).
- **SNMP-Verwendung einschränken:** Deaktivieren Sie SNMP, wenn es nicht verwendet wird. Verwenden Sie bei Bedarf SNMPv3 mit einem sicheren Passwort.
- **Deaktivieren Sie nicht benötigte Dienste:** Deaktivieren Sie alle nicht benötigten Dienste (z. B. PROFINET, ...), um potenzielle Angriffsvektoren zu reduzieren.
- **Sperren Sie ungenutzte Ports:** Deaktivieren Sie ungenutzte physische Ports mit Hilfe von Portsperrfunktionen.
- **Statische MAC-Adressen-Bindung:** Verwenden Sie MAC- oder IP-Adressbindungen, um den Netzwerkzugang zu beschränken.
- **Verwaltung von Benutzerprofilen:** Erstellen Sie mehrere Benutzerprofile mit spezifischen Rechten auf der Grundlage von Rollen.
- **Konfigurieren Sie Zugriffskontrolllisten (ACLs):** Implementieren Sie ACLs, um den Netzwerkverkehr zu kontrollieren, falls dies sinnvoll ist.

3.3.2 Router

Netzwerk-Router mit Firewall sind wichtige Komponenten für die Netzwerksicherheit, da sie den Datenverkehr kontrollieren, segmentieren und filtern können, um potenzielle Bedrohungen zu minimieren und den Schutz sensibler Ressourcen zu gewährleisten. In der Regel sind sie die Endpunkte von Conduits.

Router haben die folgenden typischen Funktionen:
Netzwerksegmentierung: Router können dazu verwendet werden um ein Netz in mehrere physische Segmente oder Subnetze zu unterteilen. Durch die Kontrolle des Datenverkehrs zwischen verschiedenen Segmenten können Router Sicherheitsrichtlinien umsetzen und den Zugang zu sensiblen Bereichen einschränken.

Firewall-Funktionen: Moderne Router verfügen über integrierte Firewall-Funktionen, die den ein- und ausgehenden Datenverkehr überwachen und filtern können. Diese Firewalls können helfen, unerwünschten Datenverkehr zu blockieren, potenziell schädliche Aktivitäten zu erkennen und zu verhindern und den Datenschutz zu verbessern, indem sie den Zugriff auf bestimmte Dienste oder Ressourcen kontrollieren

NAT (Network Address Translation): Router verwenden NAT, um private IP-Adressen im internen Netz in öffentliche IP-Adressen umzuwandeln, wenn Daten im übergeordneten Netz (oder Internet) kommuniziert werden. Dies bietet ein gewisses Maß an Sicherheit, indem es die internen Netzwerkadressen vor der direkten Offenlegung gegenüber externen Netzwerken schützt. Dies kann dazu beitragen, die Angriffsfläche zu verringern und die Privatsphäre der internen Netzressourcen zu schützen.

VPN (Virtuelles Privates Netzwerk): Router können VPN-Funktionen bereitstellen, um sichere Verbindungen zwischen entfernten Standorten oder Benutzern herzustellen. VPNs verschlüsseln den Datenverkehr und ermöglichen eine sichere Kommunikation über unsichere Netzwerke wie das Internet. So können Remote-Benutzer sicher auf Unternehmensressourcen zugreifen, ohne die Sicherheit zu gefährden.

Bewährte Security-Praktiken für Router

- Als Überblick sehen Sie sich bitte das **Video** zur sicheren Konfiguration eines Routers an.

  www.weidmueller.com/secure-router-configuration

- **Ändern Sie die Einstellungen der Firewall (Packet Filter):** Weidmüller Industrial Security Router verfügen über eine leistungsfähige Whitelisting-Firewall. Das bedeutet, dass alle Kommunikation, die nicht einer Regel von oben nach unten entspricht, verworfen wird. Die Router enthalten werksseitig eine Firewall-Regel: "Allow All". Um die Sicherheit zu verbessern, erstellen Sie eine Liste der Kommunikation, die über den Router läuft. Fügen Sie dann diese Kommunikationsparameter zu den Firewall-Einstellungen für eine Whitelist hinzu. Wenn der gesamte erforderliche Verkehr aufgelistet ist, löschen Sie die Regel "Allow All", um sicherzustellen, dass der übrige Verkehr blockiert wird.
- **Zugriffsbeschränkungen durchführen:** Weidmüller Industrial Security Routers bietet die Möglichkeit, verschiedene Benutzerprofile zu erstellen, die Rechte auf einer granularen Ebene erhalten können.
- Gewähren Sie nur denjenigen Personen Zugang, die ihn benötigen, und nur mit den Rechten, die sie für ihre Aufgaben benötigen.
- **Sichere Benutzerschnittstellen:** Deaktivieren Sie den HTTP-Zugang des Routers auf allen Schnittstellen.
- **Zugang über ein öffentliches Netz:** Deaktivieren Sie den HTTPS-Zugang des Routers auf Schnittstellen, die einem öffentlichen Netz (WAN / Mobil WWLAN) ausgesetzt sind, falls nicht erforderlich. Verwenden Sie VPN für die Kommunikation mit dem öffentlichen Netz.
- **SNMP-Nutzung einschränken:** SNMP ist standardmäßig deaktiviert. Wenn Sie es verwenden, stellen Sie bitte sicher, dass Sie SNMP v3 verwenden und ein sicheres Passwort anstelle des Standardpassworts wählen.
- **Verwenden Sie VPN für unsichere Netzwerke:** FFür den Fernzugriff auf Ihr lokales Netzwerksegment (über ein unsicheres Netzwerk) wird ein Virtual Private Network (VPN) empfohlen.
  Beim Weidmüller Security Router kann dies über eine offene Technologie wie OpenVPN oder IPsec oder den Weidmüller u-link Remote Access Service erfolgen.
- **Verwenden Sie NAT für unsichere Netzwerke:** Wenn der Router direkt mit einem öffentlichen Netzwerk verbunden ist (z. B. über 4G), aktivieren Sie NAT-Masquerading auf den Schnittstellen, um lokale IP-Adressen zu verbergen.
- Weitere Informationen im Kapitel "Fernzugriff".

3.3.3 Feldbus Netzwerk

Feldbusse wie PROFINET, EtherNet/IP, EtherCAT, Powerlink, CANopen oder Modbus sind im Hinblick auf ihre Echtzeitkommunikation auf niedrige Zykluszeiten mit geringem Jitter und Datenkonsistenz optimiert. Eine verschlüsselte Datenübertragung ist bei dieser Echtzeitübertragung nicht gegeben. Zudem werden die Konfigurationsparameter oft unverschlüsselt von der Steuerung zu unterlagerten Systemen wie Remote I/O (z.B. u-remote) übertragen.

Für das Engineering der Steuerungs- und Feldbuskonfiguration sowie für die steuerungsunabhängige Konfiguration von Feldbusgeräten werden häufig proprietäre oder Webbrowser-basierte Konfigurationstools eingesetzt. Der Zugriff auf das Gerät kann über eine separate Serviceschnittstelle oder direkt über den Feldbus erfolgen (feldbusabhängig). Weidmüller-Geräte mit Webbrowser-Oberfläche sind durch die Benutzerverwaltung vor unberechtigtem Zugriff geschützt (siehe Kapitel 3.4 Defense-in-Depth-Schicht: Komponentenzugang).

Nach dem derzeitigen Stand der Technik empfehlen wir, das Steuerungs- und Anlagennetz von anderen Netzen innerhalb einer betrieblichen Netzinfrastruktur zu trennen. Außerdem empfehlen wir eine strenge Zugangskontrolle zu solchen Maschinen- und Anlagenteilen.

Bewährte Security-Praktiken für Feldbus-Netzwerke

- **Beschränken Sie den physischen Zugang:** Sichern Sie den Zugang zu Feldbusnetzwerken mit physischen Zugangskontrollen.
- **Trennen Sie Netzwerke:** Trennen Sie das Feldbusnetzwerk von anderen Netzwerken.
- **Kleine Segmente bilden:** Segmentieren Sie große Feldbusnetze in kleinere Einheiten, um einen möglichen Cyberangriff auf einen kleineren Bereich zu beschränken.
- **Sichere Übergänge:** Kommunikationsübergänge zu anderen Zonen sollten durch Router mit entsprechend konfigurierten Firewall-Regeln gesichert werden.
- **Feste IP-Adressen verwenden:** Weisen Sie den Geräten feste IP-Adressen zu und vermeiden Sie die Verwendung von DHCP-Diensten.
- **HTTPS verwenden:** Verwenden Sie eine sichere HTTPS-Kommunikation anstelle von HTTP.
- **Deaktivieren Sie den Webserver-Zugriff über den Feldbus:** Um die Möglichkeiten von Cyberattacken zu minimieren, bieten einige u-remote-Feldbuskoppler die Möglichkeit, den Webserver-Zugriff über den Feldbus zu unterbinden. Der Webserver-Zugriff ist dann nur über USB möglich. Deaktivieren Sie, wenn möglich, den Feldbus-Webserver-Zugriff.
- **Feldbus-Dokumentation prüfen:** Beachten Sie die feldbusspezifische Dokumentation, um einen möglichst sicheren Betrieb zu gewährleisten.

3.3.4 Fernzugriffe

Der Fernzugriff ermöglicht es Benutzern, sich von einem entfernten Standort aus mit einem Netzwerk oder Gerät zu verbinden, in der Regel über ein virtuelles privates Netzwerk (VPN). Dies steigert zwar die Produktivität, indem es die Arbeit von verschiedenen Standorten aus ermöglicht, kann aber auch Sicherheitslücken mit sich bringen, wenn es nicht richtig gesichert ist.

Wichtige Überlegungen:

- Sicherheitsrisiken: Der Fernzugriff kann Angreifern die Möglichkeit bieten, sich unbefugt Zugang zu sensiblen Systemen und Daten zu verschaffen. Daher ist die Umsetzung robuster Sicherheitsmaßnahmen unerlässlich.
- Zusammenarbeit: Zwischen dem Maschinenhersteller und dem Betreiber sollte eine klare Vereinbarung über den Umfang des Fernzugriffs getroffen werden. Bei kritischen Aktivitäten sollte Personal vor Ort anwesend sein, wobei für den Zugang eine lokale Genehmigung erforderlich ist.

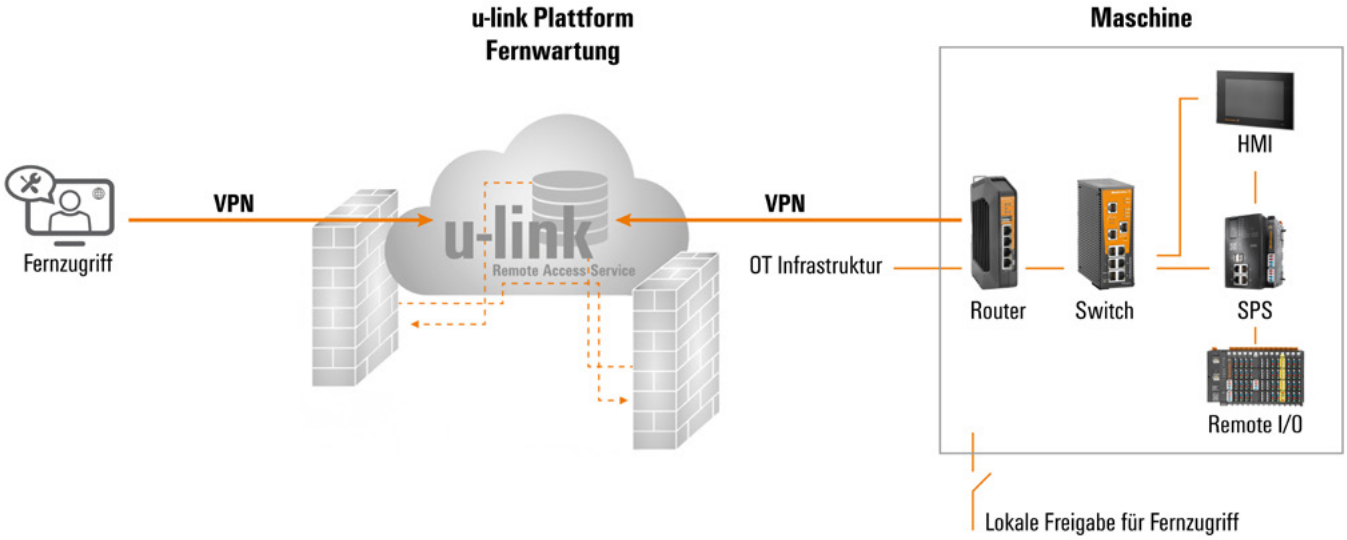

Abbildung 11 : Fernzugriffsdienst mit u-link

Weidmüller u-link System
Mit u-link bietet Weidmüller eine sichere Fernzugriffslösung an:

- Eine zentrale Cloud-Plattform
- u-link-fähige Geräte (z.B. Sicherheitsrouter, PLCs, IoT-Gateways)
- Kundenzugang über Dienstcomputer oder tragbare Geräte

Die u-link-Plattform entspricht den ISO 27001-Standards und verfügt über robuste Sicherheitsfunktionen, darunter:

- Multi-Faktor-Authentifizierung (MFA)
- Verwaltung von Benutzerrollen und -rechten
- Sichere VPN-Kommunikation
- Protokollierung von Benutzeraktivitäten

Bewährte Security-Praktiken für Fernzugriffe

- **Verwenden Sie sichere VPNs:** Implementieren Sie eine sicher verschlüsselte VPN-Verbindung, wie z. B. den Weidmüller u-link, um Daten beim Fernzugriff zu schützen.
- **Implementieren Sie die Multi-Faktor-Authentifizierung (MFA):** Erzwingen Sie MFA, um die Sicherheit von Fernzugriffsdiensten zu erhöhen. u-Link bietet Optionen für MFA.
- **Anwendung des Least-Privilege-Prinzips:** Konfigurieren Sie die Benutzerrechte so, dass die einzelnen Personen nur die für ihre Aufgabe erforderlichen Berechtigungen haben. Dazu gehört auch die Festlegung, auf welche Geräte und Ports zugegriffen werden kann.
- **Vorab-Vereinbarung über den Umfang des Fernzugriffs:** Treffen Sie eine klare Vereinbarung über den Fernzugriff zwischen dem Maschinenhersteller und dem Betreiber, bevor der Zugriff gewährt wird.
- **Lokale Autorisierung für Fernzugriff:** Verwenden Sie physische Schalter oder ähnliche Methoden, um den Fernzugriff zu erlauben oder zu verweigern. Weidmüller u-link Router verfügen über einen digitalen Eingang zur Steuerung des Fernzugriffs auf Basis einer lokalen Freigabe.
- **Systeme für Software-Updates vorbereiten:** Vergewissern Sie sich, dass sich die Maschine oder das System in einem sicheren Zustand befindet, bevor Sie Software-Updates übertragen und installieren, um die Risiken zu minimieren.

3.4 Defense-in-Depth-Schicht: Komponentenzugang

Der Informationszugang zu einem Gerät wird bei Weidmüller als User Management bezeichnet. Alternativ sind auch die folgenden Begriffe gebräuchlich:

- Access Management
- IAM (Identitäts- und Zugangsverwaltung)
- Benutzer- und Berechtigungsverwaltung / User & Permission Management

Die Benutzerverwaltung umfasst die folgenden Kernelemente:

- Identifizierung: Festlegung einer eindeutigen Identität für jeden Benutzer innerhalb des Systems (z. B. Benutzernamen).
- Authentifizierung: Überprüfung der Identität von Benutzern (z. B. durch Passwörter oder andere Überprüfungsmethoden).
- Autorisierung: Festlegung, auf welche Aktionen und Ressourcen ein authentifizierter Benutzer zugreifen kann (z. B. Berechtigungen für Konfigurationsänderungen).

Alle Weidmüller Geräte mit Webbrowser-Oberfläche verfügen über eine Benutzerverwaltung zum Schutz vor unbefugten Änderungen.
Die Berechtigungen können je nach Gerät sehr granular festgelegt werden.
Die Benutzerverwaltung ist ein entscheidendes Element für den Sicherheitsschutz und sollte entsprechend den Sicherheitsanforderungen gewissenhaft eingesetzt werden.

3.4.1 Starkes Passwort

Empfehlenswert ist eine Passwortstärke von mindestens 8 Zeichen, einschließlich Klein- und Großbuchstaben, Zahlen und Sonderzeichen.
Wir empfehlen eine Passwortlänge von mindestens 20 Zeichen bei 2 Zeichentypen zu verwenden. Wenn nur ein Zeichentyp verwendet wird, sollte die Passwortlänge mindestens 25 Zeichen betragen.

Hinweis: u-remote erfordert 3 verschiedene Zeichentypen.

3.4.2 Grundsatz der geringsten Privilegierung

Der Grundsatz der geringsten Privilegierung ist ein grundlegender Sicherheitsgrundsatz, der besagt, dass Benutzer nur die Mindestberechtigungen erhalten sollten, die sie für die Ausführung ihrer jeweiligen Aufgaben benötigen. Mit anderen Worten: Einem Benutzer sollten nur die Zugriffsrechte gewährt werden, die für die Erledigung seiner Aufgabe unbedingt erforderlich sind, und nichts darüber hinaus. Dieses Konzept dient dazu, das Sicherheitsrisiko zu minimieren, indem potenzielle Angriffsflächen reduziert werden.

In der Praxis bedeutet das Konzept der geringstmöglichen Privilegien, dass die Administratoren die Zugriffsrechte sorgfältig prüfen und nur die Berechtigungen erteilen sollten, die zur Erfüllung der Aufgaben eines Benutzers erforderlich sind. Dies erfordert eine gründliche Analyse der Rollen und Zuständigkeiten innerhalb der Organisation sowie eine regelmäßige Überprüfung und Anpassung der Berechtigungen, um sicherzustellen, dass sie aktuell und angemessen sind.

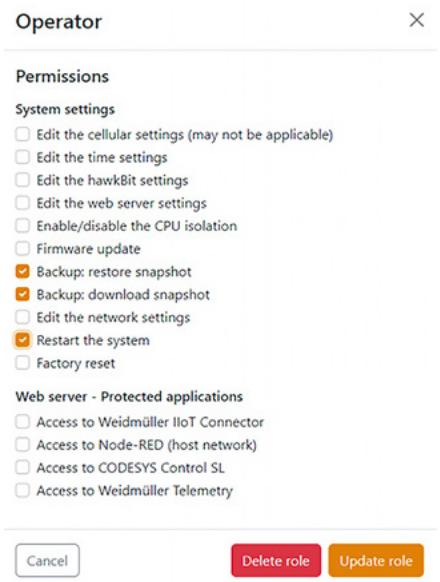

Abbildung 12 : Definition der Zugriffsrechte in u-OS

3.4.3 Browser message ‘Insecure connection’ or ‘Your connection is not private’

Wenn Sie Ihren Webbrowser mit dem Weidmüller-Gerät verbinden, erhalten Sie häufig die Browsermeldung "unsichere Verbindung", "Ihre Verbindung ist nicht privat" oder ähnliches. Dies liegt an den Sicherheitseinstellungen Ihres Browsers oder dem selbstsignierten Zertifikat auf dem Gerät.

Hier ist ein Beispiel aus einem Chrome-Browser
Der Grund für die Verwendung von selbstsignierten Weidmüller-Zertifikaten ist, dass ein Zertifikat an die verwendete IP-Adresse gebunden ist. Da diese Adresse typischerweise an die Anwendung angepasst ist, muss der Benutzer auch ein angepasstes Zertifikat ausstellen. Weitere Informationen dazu finden Sie im folgenden Kapitel.

Um mit dem Weidmüller-Gerät zu kommunizieren, klicken Sie bitte auf 'Erweitert' o.ä. und wählen Sie aus, dass Sie mit dem Gerät unsicher kommunizieren möchten.

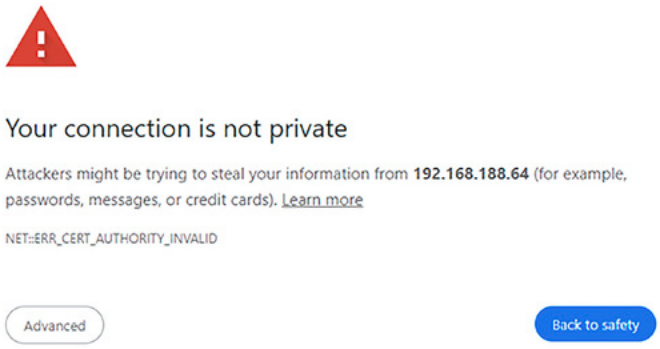

Abbildung 13 : Mögliche Browser-Meldung

3.4.4 Erstellung und Austausch von Zertifikaten

Ein Zertifikat ermöglicht eine sichere Kommunikationsverbindung mit HTTPS. Das grüne Schloss-Symbol im Browser zeigt an, dass diese Website über ein gültiges und vertrauenswürdiges Zertifikat verfügt und die Verbindung sicher ist.
Es wird empfohlen, die vorhandenen Weidmüller-Zertifikate durch eigene Zertifikate zu ersetzen.

Speziell erstellte Zertifikate sollten nach Möglichkeit von einer Zertifizierungsstelle (sog. Root-CA) signiert werden. Das Root-Zertifikat bildet den gemeinsamen Vertrauensanker für alle untergeordneten Zertifikate und muss im lokalen Truststore des Browsers bzw. Clients gespeichert werden.

Alternativ können auch selbstsignierte Zertifikate verwendet werden. Hierfür kann die XCA-Schlüsselverwaltungssoftware verwendet werden. Wichtig ist, dass die verwendete Datenbankdatei besonders geschützt ist, damit die privaten Schlüssel nicht in unbefugte Hände geraten.
Bitte wählen Sie den Schlüsseltyp RSA und die Schlüsselgröße von 4096 Bit.
Eine **Videoanleitung** zur Erstellung von selbstsignierten Zertifikaten finden Sie im Weidmüller Support Center.

www.weidmueller.com/creating-certificates

Bewährte Security-Praktiken für Komponentenzugänge

- **HTTPS-Zertifikat verwenden:** Erstellen Sie Ihr eigenes Zertifikat für die HTTPS-Kommunikation (siehe Kapitel oben).
- **Anwendung des Least-Privilege-Prinzips:** Verwenden Sie den Grundsatz der geringsten Privilegierung, der in Kapitel " 3.4.2 Prinzip des geringsten Rechtsschutzes " beschrieben wird.
- **Passwort ändern:** Ändern Sie das Standardpasswort bei der Erstkonfiguration des Geräts.
- **Verwenden Sie ein sicheres Passwort:** Bitte verwenden Sie ein sicheres Passwort, siehe Kapitel "3.4.1Starkes Passwort "
- **Verwenden Sie eindeutige Passwörter:** Verwenden Sie nicht ein Passwort für mehrere Anwendungen.
- **Individuelle Passwörter verwenden:** Empfehlenswert ist eine eindeutige Kennung (frei wählbarer Name) für jeden Benutzer.
- **Sichere Verwaltungsschnittstellen:** Aktivieren Sie den HTTPS-Zugang (deaktivieren Sie HTTP) des Geräts für Schnittstellen mit Benutzerinteraktionen.

3.5 Defense-in-depth Schicht: Software und Daten

Diese Defense-in-depth-Schicht deckt Sicherheitsthemen ab, die in einem Gerät angesiedelt sind und sich im Wesentlichen mit der Handhabung von Software und Daten befassen.

Dazu gehören:

- Firmware und ihre Aktualisierungen
- Apps und ihre Aktualisierungen
- Anwendungen
- Sichern und Wiederherstellen
- Protokollierung

3.5.1 Firmware und Updates

Weidmüller verwendet in seinen Geräten speziell industriell gehärtete Betriebssysteme und bietet Software-Updates für seine Produkte an. Bitte schauen Sie regelmäßig in unserem **Support Center** nach, ob neue Updates für Ihr Produkt verfügbar sind.

www.weidmueller.com/support-center

Updates können manuell über die Web-Benutzeroberfläche in das Gerät geladen werden.

Bei Weidmüller Security-Routern kann neue Firmware auch einfach über die zentrale u-link Cloud-Plattform auf den angeschlossenen Routern installiert werden. Dem Nutzer wird angezeigt, ob ein Update für den Router verfügbar ist. Dieses Update kann direkt oder zeitgesteuert auf dem Gerät installiert werden.

Für Geräte mit dem Betriebssystem u-OS bietet Weidmüller neben dem manuellen Update über die Weboberfläche auch eine automatisierte Update-Funktion, das sogenannte Rollout-Management, an. Das Rollout-Management ist in die Weidmüller easyConnect-Plattform integriert. Zum Einsatz kommt dabei die Open-Source-Software Hawkbit. Diese ermöglicht auch einen alternativen Serverbetrieb direkt im Unternehmensnetzwerk.

Bewährte Security-Praktiken für Firmware und Updates

- **Verwenden Sie sichere Quellen:** Achten Sie darauf, dass Sie Updates nur von vertrauenswürdigen Quellen herunterladen, z.B. Weidmüller Support Center
- **Nach Updates suchen:** Suchen Sie zyklisch nach neuen Updates für die von Ihnen verwendeten Geräte.
- **Installieren Sie Sicherheitsupdates rechtzeitig:** Installieren Sie Software-Updates und Sicherheitskorrekturen so schnell wie möglich.
- **Aktualisierungen nur im sicheren Maschinenzustand:** : Bringen Sie die Maschine oder das System vor der Aktualisierung in einen sicheren Zustand.
- **Aktualisierungen testen:** Testen Sie die neue Software, bevor Sie sie in großem Umfang installieren.
- **Servicepersonal anwesend:** Stellen Sie sicher, dass während einer automatischen Aktualisierung Servicepersonal an der Maschine oder Anlage anwesend ist, damit es im Falle eines Sicherheitsvorfalls reagieren kann.

3.5.2 Sichern und Wiederherstellen

Sicherung und Wiederherstellung sind im Zusammenhang mit einem Sicherheitsmanagementsystem aus folgenden Gründen äußerst wichtig:

- Datenwiederherstellung nach einem Sicherheitsvorfall
  Wenn ein Sicherheitsvorfall wie ein Datenverlust, ein Ransomware-Angriff oder ein Systemausfall eintritt, können Backups zur Wiederherstellung der betroffenen Daten verwendet werden. Dies minimiert den Schaden, den ein solcher Vorfall anrichten kann, und ermöglicht es den Unternehmen, den Betrieb schnell wieder aufzunehmen.
- Schutz vor Datenverlusten
  Durch regelmäßige Backups können Unternehmen sicherstellen, dass ihre Daten sicher gespeichert sind und im Falle eines Problems wiederhergestellt werden können. Dadurch wird das Risiko eines dauerhaften Datenverlusts erheblich verringert.
- Compliance-Anforderungen
  Viele Branchen und Gesetze verlangen von Unternehmen, dass sie Sicherungskopien ihrer Daten erstellen und diese für einen bestimmten Zeitraum aufbewahren, um die Integrität und Verfügbarkeit der Daten zu gewährleisten.
- Schutz vor Ransomware
  Im Falle von Ransomware-Angriffen können Backups verhindern, dass ein Unternehmen Lösegeld für die Wiederherstellung seiner Daten zahlen muss. Wenn sie über aktuelle und intakte Backups verfügen, können sie ihre Daten wiederherstellen, ohne den Angreifern nachgeben zu müssen.
- Wiederherstellbarkeit durch menschliches Versagen: Menschen machen Fehler, sei es durch versehentliches Löschen von Dateien oder unbeabsichtigte Änderungen an Daten. Backups bieten eine Möglichkeit, Daten in einem früheren Zustand wiederherzustellen und menschliche Fehler zu korrigieren.
- Geschäftskontinuität
  Backups spielen eine wichtige Rolle bei der Aufrechterhaltung der Geschäftskontinuität. Tritt ein unerwartetes Ereignis ein, das den Zugriff auf die Daten beeinträchtigt, können Backups dazu verwendet werden, den Geschäftsbetrieb aufrechtzuerhalten, während das Problem behoben wird.

Weidmüller Geräte unterstützen die Backup & Restore Funktionalität. Bitte lesen Sie die gerätespezifische Vorgehensweise im Gerätehandbuch.procedure in the device manual.

Bewährte Security-Praktiken für Sichern und Wiederherstellen

- **Regelmäßige Backups:** Führen Sie regelmäßig Backups Ihrer Geräte durch.
- **Sichere Aufbewahrung:** Bewahren Sie die Backups an einem sicheren Ort auf.
- **Langfristige Speicherung:** Bewahren Sie Backups über einen längeren Zeitraum auf. Die Malware kann das System schon viel früher infiziert haben, als der Angriff entdeckt wurde.
- **Wiederherstellungsprozess prüfen:** Überprüfen Sie die Wiederherstellungsfunktion zyklisch, um sicherzustellen, dass der Sicherungs- und Wiederherstellungsprozess funktioniert.

3.5.3 Protokollierung

Die Protokollierung ist eine wesentliche Funktion in der Sicherheitsumgebung für die Überwachung, Analyse und Reaktion auf Sicherheitsvorfälle und trägt dazu bei, die Sicherheit und Konformität von Systemen und Netzen zu verbessern.

Die Protokollierung bietet die folgenden Vorteile:

- Ereignisverfolgung:
  Protokolle bieten eine detaillierte Aufzeichnung von Ereignissen, die in einem System oder Netzwerk auftreten. Diese Ereignisse können Angriffe, unbefugte Zugriffe, fehlgeschlagene Anmeldeversuche und andere verdächtige Aktivitäten umfassen. Durch die Analyse von Protokollen können Sicherheitsteams potenzielle Sicherheitsvorfälle erkennen und auf sie reagieren.
- Forensische Analyse:
  Protokolle sind entscheidend für die forensische Analyse von Sicherheitsvorfällen. Sie ermöglichen es Sicherheitsanalysten, den Verlauf eines Angriffs zu rekonstruieren, betroffene Systeme zu identifizieren und das Ausmaß des Schadens zu bewerten.
- Einhaltung von Vorschriften:
  Viele Sicherheitsvorschriften und -standards verlangen die Protokollierung bestimmter Ereignisse und Aktivitäten. Durch die Protokollierung können Organisationen sicherstellen, dass sie die Anforderungen der Compliance-Richtlinien erfüllen.
- Frühzeitige Erkennung von Bedrohungen:
  Durch die kontinuierliche Überwachung von Protokollen können potenzielle Sicherheitsbedrohungen frühzeitig erkannt werden. Anomalien im Verhalten von Benutzern, Systemen oder Anwendungen können auf potenzielle Sicherheitsvorfälle hinweisen, die weitere Untersuchungen erfordern.
- Auditing und Nachverfolgung:
  Protokolle werden auch zur Überprüfung der Benutzeraktivitäten und des Systembetriebs verwendet. Sie ermöglichen es Organisationen, nachzuvollziehen, wer auf welche Ressourcen zugegriffen hat, welche Aktionen durchgeführt wurden und wann sie stattfanden. Dies ist wichtig, um die Integrität und Vertraulichkeit von Daten zu gewährleisten.

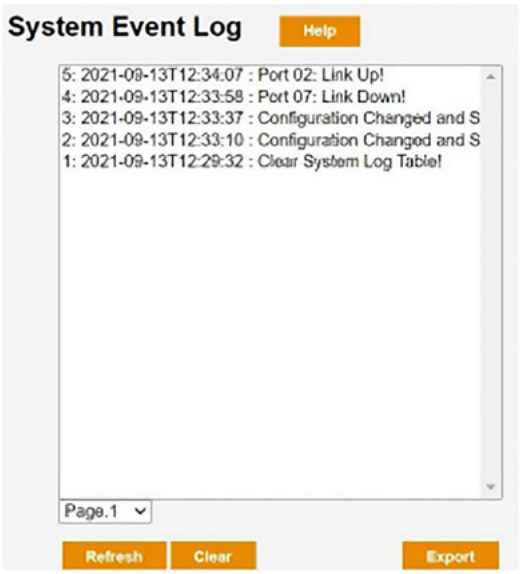

Figure 14: Beispiel Ereigniseintrag

Best Security Practices for Backup & Restore

- **Logging verwenden:** Nutzen Sie die Logging-Funktionalität in Ihrem Weidmüller Gerät (Eventlog, Ereignisprotokoll).
- **Anbindung an ein SIEM-System:** Verwenden Sie idealerweise ein zentrales SIEM-System für Ihren OT-Bereich. Aktivieren Sie die SYSLOG-Funktion in Ihrem Weidmüller Gerät und nutzen Sie eine VPN-Verbindung zum SIEM-Server (SYSLOG ist UDP-basiert).

3.5.4 u-OS Apps im Allgemeinen

3.5.4.1 APPs und Updates

Das Linux-basierte Betriebssystem u-OS für die u-control- und IoT-Gateway-Produkte ermöglicht die individuelle Erweiterung des Systems über sogenannte Docker-Container oder SSH-Zugang (SSH = Secure Shell).

Weidmüller bietet eigene und Drittanbieter-Docker-Container als fertige Apps an, die auf das Gerät geladen und ausgeführt werden können.

Für die Erstinstallation und Updates von selbst entwickelten Docker-Containern steht die App "Portainer.io" zur Verfügung. Weidmüller setzt in seinen Geräten speziell industriell gehärtete Betriebssysteme ein.

Bewährte Security-Praktiken für APPs und Updates

- **Verwenden Sie sichere Quellen:** Achten Sie darauf, dass Sie Updates nur von vertrauenswürdigen Quellen herunterladen (z.B. Weidmüller APPHUB oder Weidmüller Support Center)
- **Nach Updates suchen:** Suchen Sie zyklisch nach neuen Updates für die von Ihnen verwendeten Geräte.
- **Installieren Sie Sicherheitsupdates rechtzeitig:** Installieren Sie Software-Updates und Sicherheitskorrekturen so schnell wie möglich.
- **Aktualisierungen nur im sicheren Maschinenzustand:** Bringen Sie die Maschine oder das System vor der Aktualisierung in einen sicheren Zustand.
- **Aktualisierungen testen:** Testen Sie die neue Software, bevor Sie sie in großem Umfang installieren.
- **Servicepersonal anwesend:** Stellen Sie sicher, dass während einer automatischen Aktualisierung Servicepersonal an der Maschine oder Anlage anwesend ist, damit es im Falle eines Sicherheitsvorfalls reagieren kann.
- **Risikoanalyse:** Erstellen oder aktualisieren Sie Ihre Sicherheitsrisikoanalyse.

3.5.5 CODESYS

Die CODESYS App erweitert das u-OS Gerät um Echtzeit-Steuerungsfunktionalität sowie Echtzeit-Kommunikation mit verschiedenen Feldbussen und Kommunikation zu übergeordneten Systemen wie Servern oder Cloud-Anwendungen. Dazu gehört auch das PC-basierte Engineering mit den entsprechenden Schnittstellen zum Gerät und der CODESYS App.

Daraus ergeben sich mehrere Optionen für Sicherheitsangriffe, die in der Abbildung dargestellt sind.

CODESYS ist ein Partnerprodukt der CODESYS Group. Weitere Informationen finden Sie unter **www.codesys.com**

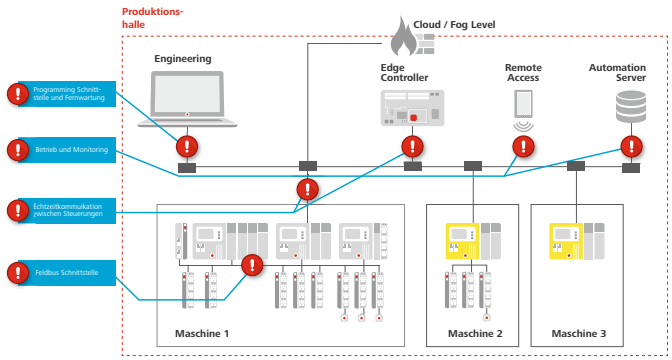

Abbildung 15 : Hauptangriffsvektoren für ein Automatisierungssystem

Das CODESYS-System bietet die folgenden Sicherheitsfunktionen:

CODESYS-Entwicklungssystem
- Verschlüsselung des Quellcodes der Anwendung mit einem Passwort, einem Dongle oder X.509-Zertifikaten.
- Benutzerverwaltung auf Projektebene
- Verschlüsselte Kommunikation zwischen dem CODESYS-Entwicklungssystem und der SPS

CODESYS Laufzeitsystem
- Benutzerverwaltung für den Zugang zum Controller
- Verschlüsselung und Signierung des ausführbaren
- Betriebsarten für den ausführbaren Anwendungscode
- Interaktive Anmeldung auf dem Zielgerät
- Einfacher Austausch oder Wiederherstellung von Controllern
- Verschlüsselte OPC UA Kommunikation

Anwendungscode
- Zugangsbeschränkungen über die Anwendung.
- Aktivieren Sie zusätzliche Funktionen. Legen Sie im Detail fest, welche Benutzer berechtigt sind, bestimmte Funktionen der Anwendung auszuführen oder zu bedienen

Visualisierung
- Benutzerverwaltung für Visualisierungen.
- Verschlüsselte Kommunikation für die CODESYS WebVisu.

CODESYS Automatisierungsserver
- Kapselung der Geräte im lokalen Netzwerk: Datenaustausch mit dem Server ausschließlich über CODESYS Edge Gateway.
- Verschlüsselte Kommunikation: Der Datenaustausch zwischen dem Server und dem CODESYS Edge Gateway erfolgt Ende-zu-Ende verschlüsselt über TLS auf Basis von X.509-Zertifikaten.
- Zuverlässige Benutzer- und Rechteverwaltung: Der Zugriff auf Objekte und Informationen kann fein abgestimmt werden, z.B. über Objekteigenschaften und Benutzerkonten - letztere zusätzlich abgesichert durch Zwei-Faktor-Authentifizierung.
- Vollständige Transparenz der Aktionen: Aufzeichnung von Zugriffen und Änderungen über Audit Trail
- Know-how-Schutz: Signierung/Verschlüsselung von Quellcode und kompiliertem Binärcode über X.509-Zertifikat, Dongle oder Passwort.
- Zertifizierte Sicherheit: Regelmäßige Sicherheitsaudits durch externe Prüfer

CODESYS-Security-Hinweise

www.codesys.com/security

3.5.6 Weidmüller Software-Werkzeuge

Weidmüller ist auch Anbieter der PROCON-Softwarefamilie und von ResMa. Diese Software-Tools können auf Windows- und Linux-Geräten von Drittanbietern installiert werden. Um einen sicheren Betrieb zu gewährleisten, müssen die folgenden Hinweise beachtet werden:

Bewährte Security-Praktiken für Weidmüller Software

- **Sichern Sie das Host-System:** Die Softwaretools PROCON-WEB SCADA und ResMa sind für den Einsatz auf Windows-Geräten konzipiert. PROCON-WEB Embedded und PROCON-Connect sind für den Einsatz unter Windows und Linux konzipiert. Das Betriebssystem muss gesichert werden, um die Integrität aller Konfigurationen und Daten, die auf dem Gerät gespeichert sind, zu gewährleisten.
- **HTTPS statt HTTP verwenden:** Im Gegensatz zu ResMa verwendet PROCON-WEB standardmäßig kein HTTPS, es wird empfohlen, HTTPS in der Konfiguration zu aktivieren, um eine verschlüsselte Kommunikation zu ermöglichen.
- **Ändern Sie die Standardkennwörter:** Ändern Sie die Standardpasswörter für Admin und Streaming direkt nach der Installation.
- **Konfigurieren Sie Richtlinien für sichere Passwörter:** TUm sichere Passwörter zu gewährleisten, stellen Sie die Passwortrichtlinien gemäß unserer Empfehlung ein, siehe Kapitel "3.4.1 Starkes Passwort"
- **Benutzerverwaltung einrichten:** Verwenden Sie die Benutzer- und Berechtigungsverwaltung bei der Erstellung einer HMI-Software. Sichern Sie Ihre HMI mit der integrierten Benutzerverwaltung und verwenden Sie Berechtigungen in Ihrem Projekt, um verschiedene Aktionen und Ansichten mit unterschiedlichen Berechtigungen zu schützen.
- **Least-Privilege-Prinzip:** Achten Sie bei der Erstellung der Berechtigungssätze für verschiedene Rollen darauf, dass nur die erforderlichen Berechtigungen zugewiesen werden.
- **Installieren Sie Security-Updates:** Wenn Weidmüller über Sicherheitslücken in der Software informiert, wird dringend empfohlen, den bereitgestellten Sicherheitspatch zu installieren.

4. Anhang

4.1 Glossar

Begriff	Erläuterung
conduit	Ein Conduit fasst die Elemente zusammen, die die Kommunikation zwischen zwei Netzwerk-Zonen ermöglichen. Conduits bieten Sicherheitsfunktionen, die eine sichere Kommunikation ermöglichen und die Koexistenz von Zonen mit unterschiedlichen Sicherheitsstufen erlauben. In der Regel wird ein Conduit durch einen Router mit einer Firewall realisiert.
CRA	**Gesetz „Cyber Resilience Act"** EU-Sicherheitsgesetz für Produkte mit digitalen Elementen und Kommunikationsfunktionen. CE-relevant Ende 2027.
CSIRT	**Computer Security Incident Response Team** Das CSIRT ist für das Schwachstellenmanagement auf Systemebene zuständig. Siehe auch PSIRT auf Produktebene.
CSMS	**Cyber Security Management System** Begriff aus der IEC 62443 für das gesamte Security Managementsystem. Der ähnliche Begriff aus der ISO27000 ist ISMS.
CSRS	Spezifikation der Cybersicherheitsanforderung.
DMZ	**Demilitarised Zone** Ein DMZ-Netzwerk ist eine zusätzliche Sicherheitsebene, die es Unternehmen ermöglicht, private Netzwerke vom öffentlichen Internetzugang zu trennen und wichtige Daten zu schützen.
DoS / DDoS	**(Distributed) Denial-of-Service-Angriff** Ein DoS-Angriff ist eine Cyber-Attacke, mit der der Angreifer verhindern will, dass Benutzer auf Netzwerk- oder Computerressourcen zugreifen können.
ENISA	Agentur der Europäischen Union für Cybersicherheit
IACS	**Industrial Automation and Control System** Begriff aus der IEC 62443. IACS bestehen aus Hardware-, Software- und Netzwerkkomponenten, die zur Automatisierung und Überwachung von industriellen Produktionsanlagen und deren Prozessen eingesetzt werden.
IDS	**Intrusion Detection System** Ein IDS erkennt anhand bestimmter Muster selbstständig Angriffe auf Computersysteme oder Netzwerke und informiert Benutzer oder Administratoren.
IEC 62443	IEC 62443 ist eine internationale Normenreihe zum Thema "Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme". Die Normenreihe ist in verschiedene Bereiche unterteilt und beschreibt sowohl technische als auch prozessuale Aspekte der industriellen Cybersicherheit. Die Reihe teilt die Industrie in verschiedene Rollen ein: die Betreiber, die Integratoren und die Hersteller.
IEC 62443-3-3	Dieser Teil der Norm IEC 62443 definiert die Systemanforderungen für ein sicheres System. Er definiert 5 Sicherheitsstufen (4 mit Sicherheitsfunktionen; Stufe 0 ohne Sicherheit).
IEC 62443-4-1	Dieser Teil der Norm IEC 62443 definiert, wie ein sicherer Entwicklungsprozess für Produkte aussehen sollte. Siehe auch SPDL.
IEC 62443-4-2	Dieser Teil der Norm IEC 62443 definiert die Produktanforderungen für ein sicheres Produkt. Er definiert 5 Sicherheitsstufen (4 mit Sicherheitsfunktionen; Stufe 0 ohne Sicherheit).
ISA 62443	Die Normenreihe der International Society of Automation (ISA) definiert Anforderungen und Verfahren für die Implementierung und Wartung elektronisch sicherer industrieller Automatisierungs- und Steuerungssysteme (IACS). Die ISA 62443 ist identisch mit der IEC 62443.
ISMS	**Information Security Management System** Begriff aus ISO 27001. Der Begriff ist gleichbedeutend mit dem Begriff CSMS in der IEC 62443.
IT	**Informationstechnologie** Abkürzung für die klassische IT-Infrastruktur wie MS Office, ERP, E-Mail, Webserver.
NIS / NIS2	**Network and Information Security** Begriff aus dem EU-Recht. NIS deckt nur kritische Infrastrukturen ab. NIS2 mit erweitertem Anwendungsbereich für viele andere Industriesegmente. NIS2 tritt mit nationalen Gesetzen in Kraft. EU-Ziel war Oktober 2024.
NIST	**National Institute of Standards and Technology** Das Institut ist eine nicht-regulatorische Behörde innerhalb des US-Handelsministeriums, die Innovationen durch die Förderung der Wissenschaft in den Bereichen Messung, Standards und Technologie vorantreibt.
NIST CSF	**NIST Cybersecurity Framework** Heute ist das NIST CSF immer noch eines der am häufigsten verwendeten Sicherheitskonzepte in der gesamten US-Industrie.
OS	Abkürzung für Operating System z.B. Weidmüller u-OS

Begriff	Erläuterung
OT	**Operational Technology** Produktionsinfrastruktur wie Produktionsmaschinen und Produktions-IT-Infrastruktur
PKI	**Public Key Infrastructure** Eine Public-Key-Infrastruktur ist ein hierarchisches System zur Erzeugung, Verteilung und Überprüfung von digitalen Zertifikaten.
PSIRT	**Product Security Incident Response Team** Das PSIRT ist für das Schwachstellenmanagement auf Produktebene zuständig. Siehe auch CSIRT auf Systemebene.
RED / RED-DA	**Radio Equipment Directive (Delegated Act)** Begriff aus dem EU-Recht. Im Allgemeinen gilt RED für Geräte mit Funkfunktionalität. Die DA-Erweiterung gilt für Security-Funktionen. RED-DA mit CE-Notwendigkeit ab August 2025.
SBOM	**Software Bill of Material** Ein SBOM dokumentiert, welche kommerziellen und freien Softwarekomponenten in Softwareprodukten enthalten sind. Es macht Abhängigkeiten von Komponenten Dritter transparent und hilft so Schwachstellen zu überwachen.
SIEM	**Security Information and Event Management** SIEM kombiniert sowohl SIM (Security Information Management) als auch SEM (Security Event Management) in einem Sicherheitsmanagementsystem. Die SIEM-Technologie sammelt Ereignisprotokolldaten aus verschiedenen Quellen, erkennt anomale Aktivitäten durch Echtzeitanalyse und leitet entsprechende Gegenmaßnahmen ein.
SL	**Security Level** Die in der IEC 62443 definierte Sicherheitsstufe beschreibt die Sicherheitsanforderungen an eine IT-Infrastruktur. SL 0: Keine besonderen Anforderungen oder Schutzmaßnahmen erforderlich. SL 1: Schutz vor unbeabsichtigtem oder versehentlichem Missbrauch. SL 2: Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln bei geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation. SL 3: Schutz gegen vorsätzlichen Missbrauch mit anspruchsvollen Mitteln, mäßigen Ressourcen, IACS-spezifischem Wissen und mäßiger Motivation. Siehe auch IACS. SL 4: Schutz gegen vorsätzlichen Missbrauch mit ausgefeilten Mitteln, umfangreichen Ressourcen, IACS-spezifischem Wissen und hoher Motivation. Siehe auch IACS.
SPDL	**Secure Product Development Lifecycle** Prozessbeschreibung aus der IEC 62443-4-1
VPN	**Virtual Private Network** Das VPN bezeichnet ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine separate physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium genutzt wird. Das VPN wird verwendet um Teilnehmer des bestehenden Kommunikationsnetzes mit einem anderen Netzwerk zu verbinden.
Zone	Netzwerkzonen unterteilen ein System in homogene Segmente, indem sie logische oder physische Systeme mit gemeinsamen Sicherheitsanforderungen gruppieren. Die Sicherheitsanforderungen werden über Sicherheitsstufen (SL) definiert.

Anmerkungen

Impressum: Weidmüller Interface GmbH & Co. KG, Klingenbergstraße 26, 32756 Detmold, Tel.: +49 5231 14280, E-Mail: weidmueller@weidmueller.de, www.weidmueller.de | Kommanditgesellschaft, Sitz: Detmold, Registergericht Lemgo HRA 2790 | Komplementärin: Weidmüller Interface Führungsgesellschaft mbH, Sitz: Detmold, Registergericht Lemgo HRB 3924, USt-IdNr.: DE124599660 | Geschäftsführer: Dr. Sebastian Durst, Dr. Timo Berger, André Sombecki, Dr. Christian von Toll

Weidmüller – Ihr Partner der Smart Industrial Connectivity

Als erfahrene Experten unterstützen wir unsere Kunden und Partner auf der ganzen Welt mit Produkten, Lösungen und Services im industriellen Umfeld von Energie, Signalen und Daten. Wir sind in ihren Branchen und Märkten zu Hause und kennen die technologischen Herausforderungen von morgen. So entwickeln wir immer wieder innovative, nachhaltige und wertschöpfende Lösungen für ihre individuellen Anforderungen. Gemeinsam setzen wir Maßstäbe in der Smart Industrial Connectivity.

Made in Germany

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
Telefon +49 5231 14-0
Telefax +49 5231 14-292083
www.weidmueller.de

Persönlichen Support
finden Sie im Internet unter:
www.weidmueller.de/kontakt

05/2025