Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

KBOB

Koordinationskonferenz der Bau- und Liegenschaftsorgane der öffentlichen Bauherren
Conférence de coordination des services de la construction et des immeubles des maîtres d'ouvrage publics
Conferenza di coordinamento degli organi della costruzione e degli immobili dei committenti pubblici
Coordination Conference for Public Sector Construction and Property Services

Empfehlung IKT-Sicherheit in der Gebäudeautomation

Stand: 1. Juli 2025; V1.0

Gebäudetechnik

Mitglieder der KBOB
BBL, armasuisse, ETH-Bereich, ASTRA, BAV, BPUK, SGV, SSV

KBOB
Fellerstrasse 21, 3003 Bern, Schweiz
kbob@bbl.admin.ch
www.kbob.admin.ch

Impressum

Ausgabe Juli 2025

Stellenwert der KBOB-Empfehlungen	KBOB-Empfehlungen legen im betreffenden Fachgebiet den generellen Standard fest, der für Objekte der KBOB-Mitglieder zur Anwendung empfohlen wird.
Herausgeber	Die Empfehlungen werden von der KBOB herausgegeben und nachgeführt. Die vorliegende Empfehlung wird von der nachfolgenden Trägerschaft unterstützt. Diese Firmen steuerten ihre Vorgängerdokumente sowie finanzielle und personelle Ressourcen zur Erarbeitung bei: • armasuisse Immobilien • BIG-EU • Bundesamt für Bauten und Logistik BBL • ETH Zürich • Flughafen Zürich AG • Insel Gruppe AG • Post Immobilien Management und Services AG • Schweizerischen Bundesbahnen AG, Infrastruktur • Swiss Re • Universitätsspital Zürich • Zoo Zürich Hinweise für Korrekturen und Ergänzungen werden gerne durch die KBOB entgegengenommen: kbob@bbl.admin.ch
Bezugsquelle	www.kbob.admin.ch/

Management Summary

Mit der zunehmenden Digitalisierung und Vernetzung von Gebäuden gewinnt die Informations- und Kommunikationstechnologie (IKT)-Sicherheit in der Gebäudeautomation (GA) stark an Bedeutung. Dies wird zunehmend auch von regulatorischen Initiativen wie NIS 2, dem Cyber Resilience Act oder den Schweizer IKT-Minimalstandards aufgegriffen.

Insbesondere Systeme der Gebäudeautomation sind in vielen Umgebungen unzureichend geschützt und bieten potenziellen Angreifern eine attraktive Angriffsfläche. Während BACnet/SC als sicherheitserweiterter Standard erste Antworten bietet, reicht ein sichereres Kommunikationsprotokoll allein nicht aus, um die Anforderungen an die IKT-Sicherheit ganzheitlich zu erfüllen.

Die vorliegende Empfehlung richtet sich an Bauherren, Betreiber und Fachplaner, die für die Sicherheit von GA-Systemen mitverantwortlich sind. Sie bietet einen praxisorientierten Leitfaden zur Integration von IKT-Sicherheitsanforderungen in bestehende und neue Gebäudeautomationssysteme – unabhängig von spezifischen Kommunikationsstandards und gewollt technologieoffen.

Im Zentrum stehen die wesentlichen organisatorischen und technischen Herausforderungen bei der Sicherung von Operational Technology (OT)-Systemen in der Gebäudeautomation. Besonderes Augenmerk gilt dabei der IT-/OT-Konvergenz, dem Mangel an standardisierten Prozessen für Software-Updates, fehlenden Zuständigkeiten sowie veralteten Systemen. Diese Faktoren führen zu einer erhöhten Angriffsfläche und erschweren die Umsetzung wirksamer Sicherheitsmassnahmen.

Das Dokument schlägt konkrete Massnahmen vor, um einen risikobasierten, holistischen Ansatz zur Steigerung der IKT-Sicherheit zu etablieren. Dies inkludiert u.a. die Etablierung eines Sicherheitsmanagementsystems gemäss des OT-Sicherheitsstandards ISA/IEC 62443-2-1, die Definition klarer Rollen und Verantwortlichkeiten, Schulungen für das involvierte Personal sowie risikobasierte Planung, Überwachung und kontinuierliche Verbesserung. Durch diese ganzheitliche Herangehensweise kann die IKT-Sicherheit in der Gebäudeautomation substanziell erhöht und die Grundlage für einen sicheren, zuverlässigen Betrieb gelegt werden.

Die Empfehlung unterstützt Bauherren dabei, die Anforderungen an die Sicherheit systematisch zu erfassen, zu bewerten und umzusetzen. Sie ist in organisatorische und technische Vorgaben gegliedert. Denn technische Massnahmen allein reichen nicht aus, um die IKT-Sicherheit in der Gebäudeautomation wirksam zu erhöhen. Erst das Zusammenspiel mit klaren organisatorischen Vorgaben – etwa zur Verantwortlichkeit, Planung, Umsetzung und Kontrolle – sowie eine enge Zusammenarbeit mit der IT-Organisation ermöglichen einen wirksamen und nachhaltigen Schutz vor Cyberbedrohungen.

Abkürzungen und Begriffe

Abkürzung	Beschreibung
AKV	Aufgaben, Kompetenzen und Verantwortungen
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
BACnet	Building Automation and Control Network
BCM	Business Continuity Management
BCP	Business Continuity Plan
CIA	Confidentiality, Integrity, Availability, auf Deutsch Vertraulichkeit, Integrität, Verfügbarkeit
CISO	Chief Information Security Officer
CSMS	Cyber Security Management System
DRP	Desaster Recovery Plan
FS-PLC	Fail Safe - Programmable Logic Controller
GA	Gebäudeautomation
IACS	Industrielle Automatisierungs- und Steuerungssysteme
IAM	Identity & Access Management
IDS	Intrusion Detection System
IKT	Informations- und Kommunikationstechnik
IPS	Intrusion Prevention System
IRP	Incident Response Plan
IP	Internet-Protokoll
ISG	Informationssicherheitsgesetz
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
ITIL	Information Technology Infrastructure Library
MitM	Man-in-the-Middle
MS/TP	Master-Slave/Token-Passing-Protokoll
NAC	Network Access Control
NIS	Netzwerk- und Informationssysteme
NIST	National Institute of Standards and Technology
NIST CSFM	NIST Cybersecurity Framework
OT	Operational Technology
OT-Security	IKT-Sicherheit in der Gebäudeautomation
RDF	Restricted Data Flow
SIEM	Security Information and Event Management / Sicherheitsinformation und -Event Management
SOC	Security Operations Center
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRE	Reaktionszeit bei Vorfällen engl. Time to Respond to Events

Referenzierte Dokumente

Titel	Autor / Herausgeber	Datum / Version	Bemerkung
[1] KBOB Empfehlung BACnet Anwendung	KBOB	2.0	Relevante KBOB Empfehlung
[2] Leitfaden zu KBOB Empfehlung BACnet Anwendung	KBOB	2.0	Relevanter Leitfaden
[3] NIST Cybersecurity Framework	NIST	2.0	Breitgenutztes Framework, u. a. die Basis der IKT-Minimalstandards des BACS
[4] ISA/IEC 62443-2-1	ISA und IEC	1.0, 2009	Weitverbreiter OT Security Standard: Dieser Teil fokussiert auf organisatorische Kontrollen
[5] ISA/IEC-62443-3-3	ISA und IEC	1.0, 2013	Weitverbreiter OT Security Standard: Dieser Teil fokussiert auf technische Kontrollen
[6] CMMI	ISACA	2.0 2018	Referenzmodell für Maturität von Organisationen, Prozessen und Kontrollen
[7] Bundesgesetz über die Informationssicherheit beim Bund	Schweizerische Eidgenossenschaft	29.09.2023	Relevantes Schweizer Gesetz
[8] ISO/IEC-27001-2022	ISO und IEC	Version 2022	Weitverbreiter IT Security Standard, auf ihm basieren sog. ISMS
[9] NIST SP 800-84	NIST	21.09.2006	Etablierte «Good Practice» für das Durchführen von IT-Übungen, z. B. Notfalltests

Inhaltsverzeichnis

Management Summary 3

Allgemeine Grundsätze zu der Empfehlung 8

1. Zum vorliegenden Dokument 9
   - 1.1. Zweck 9
   - 1.2. Abgrenzung 10
   - 1.3. Zusammenspiel mit übergeordneter Gesetzgebung 10
   - 1.4. Struktur und Verweise 10

2. Einleitung 11
   - 2.1. Gebäudeautomation (GA) und IKT-Sicherheit 11
   - 2.2. BACnet und IKT-Sicherheit 12
   - 2.3. Herausforderungen bei der Umsetzung von IKT-Sicherheit in der Gebäudeautomation 12
     - 2.3.1. OT-/IT-Konvergenz als Sicherheitsherausforderung 14

3. Generelle Anforderungen 15
   - 3.1. Planung und Bestandsaufnahme 15
     - 3.1.1. Inventarisierung 15
     - 3.1.2. Risikobewertung 15

4. Organisatorische Vorgaben 17
   - 4.1. Sicherheitsmanagementsystem 17
   - 4.2. Übersicht über die Komponenten eines Sicherheitsmanagementsystem 18
   - 4.3. Zielsetzungen für das Sicherheitsmanagementsystem anhand Maturitätslevel 19
   - 4.4. Sicherheitsrichtlinien und Verfahren 19
     - 4.4.1. Sinn und Zweck 19
     - 4.4.2. Best Practice Ansatz 19
     - 4.4.3. Praxisbeispiele 20
   - 4.5. Rollen und Verantwortlichkeiten 20
     - 4.5.1. Sinn und Zweck 20
     - 4.5.2. Best Practice Ansatz 21
     - 4.5.3. Praxisbeispiel 23
   - 4.6. Schulung und Bewusstsein 23
     - 4.6.1. Sinn und Zweck 23
     - 4.6.2. Best Practice Ansatz 24
     - 4.6.3. Praxisbeispiel 24
   - 4.7. Risikomanagement und Notfallplanung 25
     - 4.7.1. Sinn und Zweck 25

4.7.2. Best Practice Ansatz 26
4.7.3. Checkliste für Risikomanagement und Notfallplanung 27
4.7.4. Praxisbeispiel 29
4.8. Asset- und Lifecycle Management 30
4.8.1. Sinn und Zweck 30
4.8.2. Best Practice Ansatz 30
4.8.3. Checkliste für Asset- und Lifecycle-Management 31
4.9. Überwachung und Reaktion 32
4.9.1. Sinn und Zweck von Überwachung und Reaktion 32
4.9.2. Best Practice Ansatz 33
4.9.3. Praxisbeispiel 33
4.10. Schwachstellen- und Patch Management 34
4.10.1. Sinn und Zweck 34
4.10.2. Best Practice Ansatz 35
4.10.3. Praxisbeispiel 36
4.11. Audit und Bewertung 37
4.11.1. Sinn und Zweck 37
4.11.2. Best Practice Ansatz 37
4.11.3. Praxisbeispiel 39
5. Technische Vorgaben 40
5.1. Risikobasierte IKT-Sicherheitsmassnahmen, abgeleitet von Anforderungen 40
5.2. Identifikations-, Authentifikations-, und Nutzungskontrolle (AC/UC) 42
5.3. Systemintegrität (SI) 43
5.3.1. Sinn und Zweck 43
5.3.2. Best Practice Ansatz 43
5.3.3. Praxisbeispiel 45
5.4. Datenvertraulichkeit (DC) 47
5.4.1. Sinn und Zweck 47
5.4.2. Best Practice Ansatz 48
5.4.3. Praxisbeispiel 48
5.5. Eingeschränkter Datenfluss (RDF) 50
5.5.1. Netzwerkarchitektur und Netzaufteilung 50
5.5.2. Kommunikationstechnologie 55
5.5.3. Zero-Trust 55
5.6. Zeitnahe Reaktion auf Vorfälle (TRE) 56
5.7. Verfügbarkeit (Availability) von Ressourcen (RA) 58
5.7.1. Best Practice 58

Allgemeine Grundsätze zu der Empfehlung

Die vorliegende Empfehlung zur IKT-Sicherheit in der Gebäudeautomation richtet sich an alle beteiligten Akteure aus Planung, Ausführung und Betrieb. Sie dient als Orientierungshilfe für die angemessene Berücksichtigung von Sicherheitsaspekten über den gesamten Lebenszyklus von IKT-Komponenten und -Systemen in der Gebäudeautomation.

Diese Empfehlung legt den Fokus auf allgemeingültige, praxisnahe Sicherheitsprinzipien und -massnahmen im Umfeld der Gebäudeautomation, unabhängig vom verwendeten Automationsprotokoll. Sie versteht sich als Ergänzung zu bereits bestehenden technischen und betrieblichen Vorgaben – insbesondere der Empfehlung BACnet – und berücksichtigt dabei aktuelle Bedrohungslagen sowie bewährte Sicherheitsansätze.

Die Empfehlung ist grundsätzlich auf alle Objekte anwendbar. Projekt- oder nutzungsspezifische Abweichungen sowie mögliche Zielkonflikte mit bestehenden Vorgaben oder Rahmenbedingungen sind mit der Bauherrschaft bzw. den zuständigen Stellen zu klären und zu dokumentieren.

Alle Anforderungen sind hersteller- und produktneutral formuliert.

Alle aktuellen Empfehlungen, Tools und weitere Unterlagen sind unter www.kbob.admin.ch abrufbar.

1. Zum vorliegenden Dokument

1.1. Zweck

Im Dokument «KBOB Empfehlung BACnet Anwendung» [1] werden Themen behandelt, die für die Planung, Ausführung und den Betrieb von offenen, herstellerneutral ausgelegten Gebäudeautomationssystemen auf Basis von BACnet relevant sind. Werden die Empfehlungen vom Bauherren als verpflichtend eingestuft, so gelten diese als Vorgaben. Bauherrenspezifische BACnet Vorgaben können mit Hilfe des «KBOB-Leitfadens zu KBOB Empfehlung BACnet Anwendung» erstellt werden und ergänzen die Empfehlung.

BACnet ist als Standard bewusst offen und interoperabel definiert. Mit der weltweiten Vernetzung der GA wird die IKT-Sicherheit zu einem wichtigen Thema, das von jedem Bauherrn behandelt werden muss. BACnet bietet zwar mit der Erweiterung des Standards «BACnet Secure Connect» (BACnet/SC) Antworten auf gewisse Sicherheitsthemen, jedoch ist zu betonen, dass auch ein sicheres Bus-Kommunikationsprotokoll wie BACnet / SC allein nicht alle Sicherheitsprobleme löst. Die Einführung sicherer Protokolle stellt nur einen Teilaspekt eines ganzheitlichen Sicherheitskonzepts dar. Ohne zusätzliche Massnahmen wie Netzwerksegmentierung, rollenbasierte Zugriffskontrolle, Monitoring, Patch-Management und physische Sicherheit bleiben Systeme trotz sicherer Kommunikation angreifbar. Sicherheit muss systemisch gedacht werden – von der Architektur bis hin zum Betrieb – und alle Ebenen der GA- und IT-Systeme umfassen.

Damit unabhängig und übergeordnet von einzelnen Standards wie BACnet / SC oder auch KNX-Secure die IKT-Sicherheit für Gebäudeautomation definiert werden kann, bietet das vorliegende Dokument den Bauherren einen Leitfaden, um diese ergänzenden Themen zu behandeln. Die bauherrenspezifischen BACnet-Vorgaben können somit mit Hilfe des vorliegenden Dokuments um das Thema IKT-Sicherheit ergänzt werden.

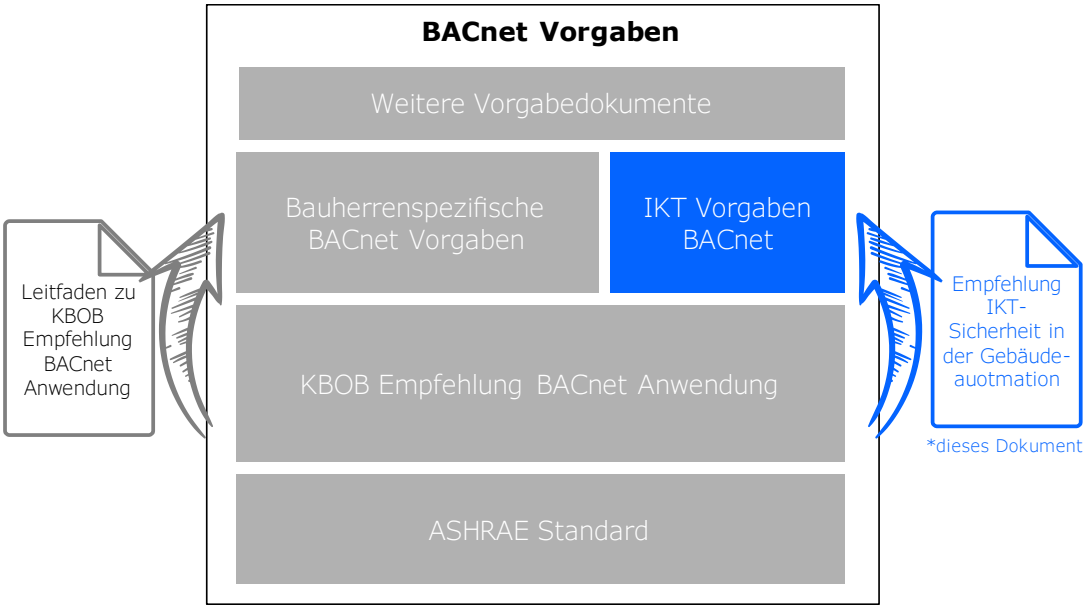

Abbildung 1: Zweck des vorliegenden Dokuments

Die IKT-Sicherheit wird in dieser Empfehlung nicht in der gesamten Breite behandelt. Stattdessen werden ausgewählte Themen aufgegriffen, die im Kontext der Gebäudeautomation und IKT-Sicherheit eine besondere Relevanz haben.

1.2. Abgrenzung

Das vorliegende Dokument dient zur Unterstützung bei der Erstellung von bauherrenspezifischen Gebäudeautomation-Vorgaben im Bereich IKT-Sicherheit. Es verfolgt bewusst einen technologie-offenen Ansatz und verzichtet auf Empfehlungen zu spezifischen Herstellern, Produkten oder Protokollen. Es werden stattdessen grundlegendere Empfehlung zur Steigerung der IKT-Sicherheit für Gebäudeautomation gemacht. Die technische Realisierung ist dann jeweils dediziert zu entscheiden.

Das Dokument enthält **keine** verbindlichen Vorgaben zur BACnet-Umsetzung.

1.3. Zusammenspiel mit übergeordneter Gesetzgebung

Nebst der schweizerischen Gesetzgebung zur Informationssicherheit [7] existieren verschiedene Gesetzgebungen der Europäischen Union, die auch einzelne Schweizer Bauherren oder deren Lieferanten betreffen können. Konkret sind hier NIS 2 und der Cyber Resilience Act (CRA) zu nennen. Dieses Dokument thematisiert diese EU-Gesetzgebung gewollt nicht und macht keine Aussagen für deren Anwendbarkeit für Bauherren oder die an sie gestellten Anforderungen. Die Anwendbarkeit und die damit verbundenen Anforderungen müssen Bauherren selbst prüfen. Besonders im Zusammenhang mit dem CRA ist die enge Zusammenarbeit mit Lieferanten und Kunden erforderlich und sollte daher besondere Aufmerksamkeit erhalten.

Gleichwohl sei angemerkt, dass die im Dokument referenzierten Standards ISO/IEC-27001 [8] und ISA/IEC-62443 [4][5] auch in der EU weit verbreitet sind und industrieübergreifend als «Good Practice» zur Erhöhung der IKT-Sicherheit gelten.

1.4. Struktur und Verweise

Das Dokument behandelt IKT-Themen in der Struktur von gängigen IKT-Richtlinien. Pro Thema werden Teilbereiche aufgegriffen und ein Bezug zu BACnet / Gebäudeautomation hergestellt. Zusätzlich werden Empfehlungen gegeben, wie die bauherrenspezifischen BACnet-Vorgaben ergänzt werden können.

Damit eine Verbindung zu den bereits bestehenden Dokumenten ersichtlich ist, bedient sich das Dokument von Verweisen.

Beispiel:

à [1], Kap. 5.2.1., S. 20: Verweis auf Dokument [1], Kapitel 5.2.1., Seite 20

2. Einleitung

2.1. Gebäudeautomation (GA) und IKT-Sicherheit

Die Gebäudeautomation gehört zur Kategorie der «Operational Technology» (OT) und unterscheidet sich damit grundlegend von der klassischen «Information Technology» (IT).

Während IT-Systeme primär auf Datenverarbeitung, Bürokommunikation und Unternehmensprozesse ausgerichtet sind, fokussiert sich OT auf die Überwachung, Steuerung und Automatisierung physischer Prozesse – im Fall der Gebäudeautomation also auf gebäudetechnische Anlagen und Systeme.

Aufgrund ihrer zentralen Rolle sind OT-Systeme zunehmend Ziel von Cyberangriffen. Bedrohungen können die Verfügbarkeit, Integrität und Vertraulichkeit dieser Systeme gefährden und im Ernstfall erhebliche Auswirkungen auf die betroffenen Organisationen haben – etwa durch Betriebsunterbrüche, Sicherheitsrisiken oder wirtschaftliche Schäden.

Trotz der funktionalen Unterschiede zwischen IT und OT ist eine koordinierte Verbindung beider Bereiche essenziell. Ein technologieoffener Ansatz hilft dabei, Sicherheitslücken zu vermeiden und gleichzeitig die Betriebssicherheit sowie Verfügbarkeit der OT-Systeme zu gewährleisten. Dabei gilt es, sowohl die IKT-Sicherheitsanforderungen der IT als auch die Betriebssicherheitsanforderungen der OT angemessen zu berücksichtigen.

Zu den Cyberbedrohungen zählen Schadsoftware wie Viren, Würmer und Trojaner, welche OT-Systeme infizieren, Daten stehlen oder zerstören und den Betrieb stören können. Ransomware-Angriffe, bei denen Angreifer Daten verschlüsseln oder den Zugriff auf kritische Systeme blockieren, um Lösegeld zu fordern, sind ebenfalls eine erhebliche Gefahr. Langfristige, gezielte Angriffe durch gut organisierte und oft staatlich geförderte Gruppen, die sich Zugang zu sensiblen OT-Systemen verschaffen und diese überwachen oder manipulieren, stellen eine weitere bedeutende Bedrohung dar.

Menschliche Bedrohungen umfassen sowohl innere Bedrohungen durch unzufriedene oder korrupte Mitarbeitende, die absichtlich Schaden anrichten, als auch unabsichtliche Fehler, die durch Fehlbedienungen oder mangelnde Schulung des Personals entstehen können. Ebenso können Mitbewerber innerhalb eines Projekts – wie beispielsweise Inbetriebnehmer anderer Unternehmen – oft unbemerkt Schäden anrichten, etwa durch Änderungen an Regelparametern eines Controllers, durch Deaktivieren der Kommunikation mit Device Communication Control oder durch eine falsche Zeitsynchronisation. Auch physische Bedrohungen wie Sabotage und Diebstahl können den Betrieb erheblich stören. Direkte physische Angriffe auf OT-Systeme oder der Diebstahl von Hardware und vertraulichen Informationen können zu schweren Betriebsunterbrechungen und Datenverlusten führen. Zudem sind OT-Systeme auch durch Umgebungsbedrohungen wie Naturkatastrophen gefährdet. Ereignisse wie Erdbeben, Überschwemmungen oder Stürme können physische Schäden an der Infrastruktur verursachen. Technische Ausfälle durch Hardware- oder Softwarefehler können ebenfalls zu unerwarteten Betriebsunterbrechungen führen.

Ein besonderes Risiko geht von veralteten Systemen und Software aus, die nicht mehr aktualisiert werden und daher anfällig für bekannte Sicherheitslücken sind. Schwache Authentifizierungs- und Autorisierungsmechanismen erleichtern unbefugten Zugriff auf OT-Systeme. Zudem erhöht die mangelnde Netzwerksegmentierung zwischen OT- und IT-Netzwerken die Angriffsfläche erheblich. Unsichere Fernzugriffslösungen bieten einfache Einstiegspunkte für Angreifer. Die zunehmende Vernetzung und Integration von OT mit IT-Systemen schafft zusätzliche Angriffspunkte durch erhöhte Komplexität und Interoperabilität.

Die Eintrittswahrscheinlichkeit dieser Bedrohungen ist hoch, insbesondere in einer zunehmend digitalisierten und vernetzten Welt. Die Auswirkungen können erheblich sein, da OT-Systeme direkte physische Prozesse steuern und überwachen. Ein erfolgreicher Angriff kann nicht nur zu finanziellen Verlusten, sondern auch zu erheblichen Sicherheitsrisiken für Mitarbeitende und die Öffentlichkeit führen.

2.2. BACnet und IKT-Sicherheit

Obwohl BACnet als Kommunikationsprotokoll für Gebäudeautomations- und Steuerungsnetzwerke weit verbreitet ist und viele Vorteile bietet, reicht es allein nicht aus, um den umfassenden Schutz zu gewährleisten, den moderne OT-Systeme benötigen. BACnet wurde ursprünglich mit dem Fokus auf Interoperabilität und Effizienz entwickelt und nicht primär mit Blick auf die heutigen komplexen Cyberbedrohungen. Es fehlen oft integrierte Sicherheitsmechanismen wie starke Authentifizierung, Verschlüsselung und detaillierte Zugriffskontrollen. Aufgrund dieser Schwächen bieten BACnet-Empfehlungen allein nicht ausreichend Schutz gegen die vielfältigen Bedrohungen, denen OT-Systeme ausgesetzt sind.

BACnet bietet zwar mit der Erweiterung des Standards (BACnet/SC) Antworten auf gewisse Sicherheitsthemen, jedoch wird die Erweiterung in diesem Dokument explizit ausgeklammert (Kapitel 1).

Aufgrund seiner offenen Struktur ist BACnet/IP aus Sicht der IKT-Sicherheit mit besonderer Aufmerksamkeit zu betrachten.

Deshalb sind zusätzliche Sicherheitsmassnahmen und -empfehlungen unerlässlich, um ein höheres Mass an Sicherheit zu gewährleisten. Diese umfassen unter anderem technische Massnahmen wie die Implementierung von Multi-Faktor-Authentifizierung, regelmässige Sicherheitsupdates und Patches, Netzwerksegmentierung, sichere Fernzugriffslösungen als auch organisatorische Massnahmen wie umfassende Schulungs- und Sensibilisierungsprogramme für Mitarbeitende. Durch die Integration dieser erweiterten Sicherheitsmassnahmen können Unternehmen ihre OT-Systeme besser vor Angriffen schützen und die Betriebskontinuität sicherstellen. Nur durch eine Kombination von Gebäudeautomation und zusätzlichen Sicherheitsmassnahmen kann ein robustes Sicherheitsniveau erreicht werden, das den modernen Bedrohungen angemessen begegnet.

Mit der Umsetzung von Massnahmen, die unter anderem in diesem Dokument empfohlen werden, kann das Risiko, welches BACnet als Protokoll mit sich bringt, nur bedingt reduziert werden. Somit müssen weitere Sicherheitsmassnahmen umgesetzt werden, welche sich nicht nur auf das Protokoll beziehen, sondern auch andere Teile der Gebäudeautomation oder IT im Allgemeinen betreffen.

2.3. Herausforderungen bei der Umsetzung von IKT-Sicherheit in der Gebäudeautomation

Eine wesentliche Herausforderung bei der Umsetzung von IKT-Sicherheit in der Gebäudeautomation ist die Überbrückung des „Gaps“ zwischen Information Technology (IT) und Operational Technology (OT). Während IT-Systeme auf Datensicherheit und kurze Innovationszyklen ausgerichtet sind, stehen in der OT-Prozessstabilität, Effizienz und lange Lebenszyklen im Vordergrund.

In der Gebäudeautomation werden Prinzipien verfolgt, die sich nur schwer mit den Grundsätzen der IKT-Sicherheit in Einklang bringen lassen:

- Lifecycle in der Gebäudeautomation: Der Lebenszyklus von Geräten in der Gebäudeautomation ist im Normalfall deutlich länger als in der IT, oft über 5 bis 20 Jahre. Dies erschwert die regelmässige Implementierung von Sicherheitsupdates und stellt besondere Anforderungen an das Lifecycle-Management.
- Softwareupdates und Patches: Standardisierte Prozesse zur Durchführung von Softwareupdates und Patches sind häufig nicht vorhanden. Zudem wird meist nicht garantiert, dass GA-Geräte über ihren gesamten Lebenszyklus hinweg mit Sicherheitsupdates versorgt werden, was sie anfällig für bekannte Schwachstellen macht.
- IT-/OT-Konvergenz: Die Kombination von Gebäudeautomation und IT kann die Sicherheit der Infrastruktur sowohl verbessern als auch zusätzliche Risiken mit sich bringen. Eine erfolgreiche Integration ermöglicht zwar eine verbesserte Sicherheitsüberwachung und eine schnellere Reaktion auf Bedrohungen, stellt jedoch gleichzeitig neue Herausforderungen in Bezug auf die Sicherheit dar. Diese Herausforderungen werden im Kapitel 0 näher beschrieben und erfordern gezielte Massnahmen zur Risikominderung.
- Verantwortlichkeiten: Die klare Definition und Verteilung von Verantwortlichkeiten sind entscheidend, um sicherzustellen, dass IT- und OT-Teams gemeinsam an der Gewährleistung der Sicherheit arbeiten. Ohne klar festgelegte Zuständigkeiten besteht die Gefahr von Sicherheitslücken und ineffizienten Prozessen.

Die Liste ist nicht abschliessend und soll lediglich die wichtigsten Herausforderungen auflisten.

Die folgende Grafik verdeutlicht die Unterschiede zwischen IT und OT und zeigt die Notwendigkeit, diese Unterschiede durch gezielte Massnahmen zu überbrücken. Die Abbildung spiegelt die heutige Ist-Situation typischerweise wider, ist jedoch nicht abschliessend und darf nicht als Soll-Zustand verstanden werden.

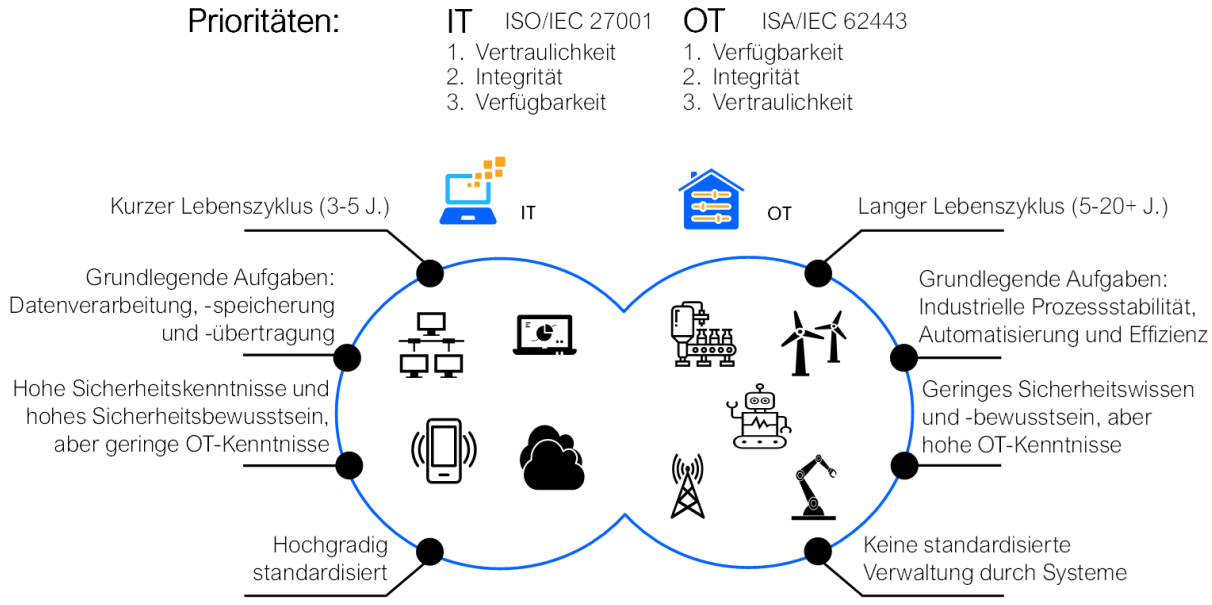

Abbildung 2: Unterschiede zwischen IT und OT

2.3.1. OT-/IT-Konvergenz als Sicherheitsherausforderung

Mit der zunehmenden Konvergenz von IT- und OT-Systemen verschmelzen vormals getrennte technologische Welten. Diese Entwicklung bringt zwar viele Vorteile wie Effizienzsteigerung, verbesserte Analysefähigkeiten und zentralisiertes Monitoring – gleichzeitig entstehen dadurch neue, teils gravierende Risiken.

Durch die Verbindung von IT-Infrastrukturen mit operativen Systemen der Gebäudeautomation erweitern sich die Angriffsflächen deutlich: IT-typische Bedrohungen wie Malware, Ransomware oder gezielte Remote-Angriffe können nun auch auf OT-Systeme übergreifen, die ursprünglich nicht für solche Szenarien ausgelegt waren. Damit steigt nicht nur die Wahrscheinlichkeit eines Angriffs, sondern auch das potenzielle Schadensausmass – etwa durch den Ausfall kritischer Infrastrukturen, Manipulation physischer Prozesse oder längerfristige Betriebsunterbrüche.

Diese Entwicklung erfordert neue Sicherheitsstrategien, die beide Welten gleichermassen berücksichtigen. Schutzmassnahmen müssen über Systemgrenzen hinweg geplant und umgesetzt werden – vom Endgerät bis zum Leitsystem, vom Sensor bis zur Cloud. Sie müssen technologieoffen und flexibel sein und gleichzeitig den spezifischen Anforderungen der OT-Welt gerecht werden – wie Echtzeitverarbeitung, geringe Ausfalltoleranz und lange Lebenszyklen der Geräte.

Ein zentrales Problem stellen dabei fehlende oder unklare Verantwortlichkeiten an den Schnittstellen zwischen IT und OT dar. In der Praxis führt dies oft zu unkoordinierten Zuständigkeiten und somit zu erhöhtem Risiko.

Ein Sicherheitskonzept, das sowohl IT- als auch OT-Risiken gemeinsam berücksichtigt, ist deshalb unabdingbar.

3. Generelle Anforderungen

3.1. Planung und Bestandsaufnahme

Bevor Massnahmen zur Verbesserung der OT-Security (IKT-Sicherheit in der Gebäudeautomation) ergriffen werden, ist es entscheidend, alle Geräte und Systeme im Gebäudeautomationsnetzwerk zu erfassen und ihre jeweiligen Risiken zu bewerten.

3.1.1. Inventarisierung

Bei der Inventarisierung wird eine vollständige Liste aller Geräte, Systeme und relevanten Komponenten im Gebäudeautomationsnetzwerk (GA-Netz) erstellt. Dabei sind nicht nur Endgeräte wie Sensoren, Aktoren oder Steuerungen zu erfassen, sondern auch alle Netzwerkkomponenten wie Switches, Router und Firewalls. Ebenfalls zu berücksichtigen sind Übergänge zwischen OT- und IT-Netzwerken, Fernzugriffe (z. B. via VPN) sowie Internet Breakouts. Falls in der Umgebung IoT-Geräte oder dedizierte IoT-Netzwerke für OT-Systeme eingesetzt werden, sind auch diese entsprechend zu inventarisieren.

Die Inventarisierung umfasst mindestens folgende Merkmale:

- Typ und Kategorie der Geräte oder Systeme (z. B. Sensoren, Aktoren, Steuerung, Netzwerkkomponente, IoT-Gerät)
- Verwendungszweck (z. B. HVAC, Zugangskontrolle, Videoüberwachung, Netzwerkweiterleitung)
- Verbindungsarten (z. B. kabelgebunden, drahtlos, mobilfunkbasiert) Netzwerkeinstellungen (z. B. IP-Adresse, MAC-Adresse, benötigte Ports, VLAN-Zugehörigkeit)
- Standort und physische Verteilung
- Firmware- und Software-Versionen
- Vorhandene Zertifikate, insbesondere bei verschlüsselten oder sicherheitsrelevanten Geräten (z. B. TLS-Zertifikate, FDSK-Schlüssel)

Die Inventarisierung bildet die Grundlage für weitere Sicherheits- und Managementmassnahmen und ist eng mit dem Kapitel 4.8 Asset- und Lifecycle Management verknüpft. Dort sind Prozesse zur kontinuierlichen Pflege, Aktualisierung und Ausmusterung der inventarisierten Komponenten festgelegt.

Die Liste der zu erfassenden Elemente sollte in einer geeigneten, flexibel erweiterbaren Form geführt werden, um auch zukünftige Technologien und Gerätetypen berücksichtigen zu können.

3.1.2. Risikobewertung

Bei der Risikobewertung werden Risiken für jeden Gerätetyp und jedes System identifiziert und hinsichtlich der Kritikalität und der möglichen Auswirkungen eines Sicherheitsvorfalls bewertet. Dies umfasst:

- Schwachstellenanalyse (z. B. bekannte Sicherheitslücken, potenzielle Angriffsvektoren, fehlende Sicherheitsfunktionen)
- Bewertung der Kritikalität des jeweiligen Gerätetyps bzw. Systems für den sicheren und stabilen Betrieb

- Analyse der potenziellen Auswirkungen bei Ausfall, Manipulation oder unautorisiertem Zugriff
- Klassifizierung der Geräte und Systeme nach Schutzbedarf (z. B. hoch, mittel, niedrig)

Die Risikobewertung dient als Grundlage für die Priorisierung von Schutzmassnahmen und sollte regelmässig aktualisiert werden – insbesondere bei Systemänderungen, neuen Bedrohungslagen oder nach relevanten Vorfällen.

4. Organisatorische Vorgaben

Dieses Kapitel beschäftigt sich mit organisatorischen Aspekten der Steigerung der IKT-Sicherheit für die Gebäudeautomation. Es bedient sich hier der weitverbreiteten «Good Practices» des ISA/IEC-62443-2-1 Standards [4].

Es beginnt mit dem Überbau der Arbeiten zugunsten IKT-Sicherheit in Kapitel 4.1 in der Form eines Sicherheitsmanagementsystems, sowie einem Einblick in dessen risikobasierte und risikoorientierte Funktionsweise in Kapitel 4.2 und die zielführende pragmatische Zielsetzung entlang Maturitätslevels (Kapitel 4.3). Um ein derartiges Programm zu etablieren, bedarf es die Definition und Etablierung von notwendige Sicherheitsrichtlinien und Verfahren (Kapitel 4.4) sowie die klare Abklärung der Rollen und Verantwortlichkeiten innerhalb einer Organisation zugunsten der IKT-Sicherheit (Kapitel 4.5). Mitarbeitende in der Gebäudeautomation verfügen oft nur über begrenzte Praxiserfahrung im Bereich IKT-Sicherheit. Durch gezielte Schulungen und Sensibilisierungsmassnahme (Kapitel 4.6) werden sie entsprechend befähigt und für sicherheitsrelevante Aspekte sensibilisiert. Um mit IKT-Sicherheitsrisiken umgehen zu können und sich proaktiv gegen Sicherheitsvorfällen vorzubereiten, bedarf es eines Risikomanagements sowie zielführender Notfallplanung (Kapitel 4.7). Die Basis für die technischen Massnahmen aus Kapitel 5 ist ein funktionierendes Asset- und LifeCycle Management (Kapitel 4.8). Um Sicherheitsvorfälle zu erkennen, wenn sie passieren, bedarf es Überwachung und geeignete Reaktionsmassnahmen (Kapitel 4.9). Um Sicherheitsvorfälle zu adressieren, bevor sie passieren, braucht es ein Schwachstellen- und Patch-Management (Kapitel 4.10). Abschliessend, um die Effektivität und Umsetzung der Massnahmen bewerten zu können, sowie den kontinuierlichen Verbesserungsprozess zu etablieren, braucht es ein geregeltes Audit-, Assessment- und Bewertungsprogramm (Kapitel 4.11).

4.1. Sicherheitsmanagementsystem

Um die IKT-Sicherheit der Gebäudeautomation koordiniert und gesamtheitlich über die sämtlichen Dimensionen wie Prozesse, Strukturen und Technologie sicherzustellen, ist die Nutzung eines Sicherheitsmanagementsystems (auch: Sicherheitsmanagementprogramm) empfohlen. Hier gibt es klassischerweise für die Informationstechnologie (IT) das bekannte Information Security Management System (ISMS), basierend auf der ISO27001 Normreihe. Für die Gebäudeautomation als sogenannte Operative Technologie (OT) gibt es das so genannte Cyber Security Management System (CSMS) basierend auf der ISA/IEC-62443 Normreihe.

Diese zwei Normenreihen werden explizit zwischen den drei involvierten Organisationen ISO, ISA und IEC abgestimmt, um miteinander kompatibel zu sein. Dies ist auf technischer Ebene im Kontext der voranschreitenden Konvergenz von IT (Server, Cloud-Dienste) und OT (industrielle Kontrollsysteme) sinnvoll. Es erlaubt aber auch Organisationen auf der prozeduralen und organisatorischen Ebene, bereits existierende Prozesse, Richtlinien und Strukturen aus dem ISMS auch auf ihre OT zu erweitern. Wenn eine Organisation zum Beispiel für ihre IT schon einen funktionierenden Business Continuity Management (BCM) Prozess hat, kann sie diesen auch direkt auf die OT erweitern, wobei der ISA/IEC-62443 Standard sie dabei explizit unterstützt.

Entscheidend für den Erfolg eines Sicherheitsmanagementsystem ist die Unterstützung für das Programm durch die Geschäftsleitung oder dem Management. Hierfür empfiehlt der OT-Sicherheitsstandard ISA/IEC-62443-2-1 [4] die Entwicklung einer geschäftlichen Grundlage für das Sicherheitsmanagementsystem, die klare Definition seines Geltungsbereichs sowie die Einbeziehung aller relevanter Stakeholder. Dies erlaubt die proaktive Etablierung und Umsetzung des Sicherheitsmanagementsystem als fester Bestandteil des geschäftlichen Vorgehens.

Nach ISA/IEC-62443-2-1 [4] ist dabei die Basis eines erfolgreichen Sicherheitsmanagementsystem die Risikobewertung des sogenannten «System under Scope», im Fall der Gebäudeautomation also das relevante Gebäude oder die relevante Anlage. Dieses System inkludiert nebst den technischen Komponenten auch die verschiedenen Geschäftsprozesse, Organisationstrukturen und das Personal. Die Risikobewertung inkludiert

1) die Identifikation relevanter Risiken

2) die Erfassung und Priorisierung der Systeminventars nach Schutzbedarf

3) Zuweisung der Risiken auf Schutzobjekte

4) die Priorisierung der Risiken

Dies erlaubt dem Sicherheitsmanagementsystem die qualifizierte Bestimmung und Zuweisung von Sicherheitsmassnahmen und -Technologien und liefert den Beurteilungskontext bei der späteren Entwicklung der Gefahrenlage. Diese Sicherheitsmassnahmen und -Technologien erleben dann eine regelmässige Qualitäts- und Wirksamkeitskontrolle zur kontinuierlichen Aufrechthaltung des Sicherheitsmanagementsystem. Die Risikobewertung selbst sollte auch regelmässig überprüft und überarbeitet werden, wodurch sich Handlungsbedarf und Anpassungen an den Massnahmenkatalog ergeben.

4.2. Übersicht über die Komponenten eines Sicherheitsmanagementsystem

Damit ergibt sich ein Sicherheitsmanagementsystem aus dem Kreislauf von Risikoerfassung, -behandlung und -überprüfung.

Unter der Grosskomponente «Risikoerfassung» fallen dabei der kontinuierliche Einbezug des geschäftlichen Kontextes, die Verwaltung des sogenannten «Asset-Inventars» der IKT-Objekte und – Dienste (z.B. GA-Steuerungsgeräte, die gesteuerten Geräte wie Lüftung oder Beleuchtung, sowie die Steuerungsprogramme) sowie die Risikobewertung des Inventars. Dies inkludiert auch Teile des Schwachstellen- und Patch-Managements durch die Identifizierung und Bewertung neuer Schwachstellen und Patches, die für Komponente des Systems relevant sind. Dies stimmt grossteilig mit den Funktionen «Identify» und «Govern» des NIST CSF [3] überein.

Unter der Grosskomponente «Risikobehandlung» fallen dann die Identifikation und Umsetzung von verschiedenen Massnahmen und Technologien, welche man grundsätzlich aufteilen kann in organisatorische, prozedurale und technische Aspekte. Unter den organisatorischen Aspekt verordnen sich dabei Themen wie Etablierung der Sicherheitsorganisation, Definition von IKT-Sicherheitsvorgaben und -richtlinien sowie Aktivitäten zur Schulung der Mitarbeitenden, aber auch die Notfallplanung. Unter dem prozeduralen Aspekt verordnen sich Themen wie Asset Management, Patch Management, Change Management und Incident Management. Abschliessend verordnen sich unter dem technischen Aspekt Themen wie Zugriffs- und Nutzungskontrollen, Netzwerksegmentierung und Systemüberwachung. Im NIST CSF [3] wären dies die Funktionen «Govern», «Protect», «Detect», «Respond» und «Recover».

Unter der Grosskomponente «Risikoüberprüfung» fallen die Aktivitäten zur kontinuierlichen Überprüfung und Verbesserung des Sicherheitsmanagementsystem. Dies inkludiert Themen wie die Auditierung und Bewertung von umgesetzten Massnahmen, die Anpassung der Risikobewertung basierend auf der aktuelle Gefahrenlage sowie der Einarbeitung des Feedbacks der verschiedenen Stakeholder. Dies lässt sich unter der Funktion «Govern» des NIST CSF [3] einordnen.

4.3. Zielsetzungen für das Sicherheitsmanagementsystem anhand Maturitätslevel

Dieses Dokument empfiehlt, wie auch der Standard ISA/IEC 62443-2-1 [4], dass die Zielwerte für das gesamte Sicherheitsmanagementsystem entweder einheitlich festzulegen oder aufgeteilt für die verschiedenen Teile des Sicherheitsmanagementsystem das Prozess-Maturitätsmodell von CMMI [6] zu verwenden. Dies definiert anhand einer aufsteigenden Skala von 1 bis 5 die Maturität oder den Reifegrad von Prozessen oder eines Programms. Es beginnt bei einem ad hoc und undokumentierten Prozess, über einen statischen, tool-gestützten Prozess hin zu einem dynamischen und kontinuierlichen verbesserten Prozess.

Als Beispiel dient hierfür die Massnahme «IKT-Sicherheitsschulungen der Mitarbeitenden». Bei einem Maturitätslevel von 1 finden diese nicht standardmässig statt und werden nur reaktiv bei einem Vorfall für einzelne Personen nachgeholt. Bei einem Maturitätslevel von 3 gibt es eine statische Standardschulung zum Thema «IKT-Sicherheit», welche in einer definierten Frequenz für alle Mitarbeitenden durchführt wird. Bei einem Maturitätslevel von 5 nutzt die Organisation eine statische Kontrolle, um die Qualität und Wirkung der Schulungen zu erfassen und zu testen, wodurch sie die Schulung kontinuierlich verbessert.

Die Auswahl des angestrebten Maturitätslevels für das Sicherheitsmanagementsystem und dessen Komponenten sollte risikobasiert, kontextbezogen und geschäftsorientiert erfolgen. Ein Soll-Wert von 3 wird dabei häufig als Ziel definiert, höhere Zielwerte sind seltener. Der Ist-Zustand liegt oft lediglich bei Stufe 1 oder 2. Es empfiehlt sich dementsprechend im Kontext von Budget und personellen Ressourcen der Sicherheitsorganisation realistische und erreichbare Zielwerte zu definieren und diese im Sinne eines kontinuierlichen Verbesserungsprozesses schrittweise bei Bedarf zu erhöhen.

4.4. Sicherheitsrichtlinien und Verfahren

Eine Richtlinie legt den grundsätzlichen Rahmen und die Zielsetzung fest, während ein Verfahren detailliert beschreibt, wie diese Vorgaben in der Praxis umzusetzen sind.

4.4.1. Sinn und Zweck

Sicherheitsrichtlinien für die Gebäudeautomation sollten auf bereits vorhandene, übergeordnete Vorgaben basieren und die identifizierten Risiken angemessen berücksichtigen. Auf dieser Grundlage werden konkrete OT-Security-Verfahren definiert, die beschreiben, wie die Richtlinien praktisch umzusetzen sind. Sicherheitsrichtlinien und -verfahren müssen entwickelt, erfolgreich eingeführt und dauerhaft aufrechterhalten werden, um ein angemessenes Mass an IKT-Sicherheit in der Gebäudeautomation zu gewährleisten.

Die schriftlich festgelegten Richtlinien und Verfahren gewährleisten, dass während der gesamten Betriebsdauer der Gebäudeautomation die Sicherheitsziele Verfügbarkeit, Integrität und Vertraulichkeit erfüllt bleiben. Zugleich vermitteln sie Mitarbeitenden, Auftragnehmenden, Dritten sowie anderen relevanten Interessengruppen ein eindeutiges Bild von den Cybersecurity-Grundsätzen des Unternehmens und verdeutlichen ihre jeweiligen Rollen und Zuständigkeiten beim Schutz der betrieblichen Werte.

4.4.2. Best Practice Ansatz

Die Sicherheitsrichtlinien und Verfahren müssen spezifischen Anforderungen an die IKT-Sicherheit in der Gebäudeautomation klar festlegen. Zum Beispiel kann eine Richtlinie vorschreiben, dass Zugriffsrechte auf GA-Systeme nach einem rollenbasierten Modell

vergeben werden. Nur autorisierte Personen dürfen Zugriff erhalten. Diese Rechte müssen regelmässig überprüft und bei Bedarf angepasst werden, insbesondere bei Veränderungen im Personal.

Ein weiteres Beispiel ist die Vorgabe, dass Netzwerke in der Gebäudeautomation logisch segmentiert werden müssen. Kritische Systeme, wie die Steuerung von Sicherheitsanlagen, sollen dabei strikt von anderen Netzwerken getrennt sein, um die Auswirkungen potenzieller Angriffe zu minimieren. Die Umsetzung erfolgt über detaillierte Verfahren, welche die Einrichtung und Überwachung der Segmentierung genau beschreiben (Kapitel 5.5).

Als Best Practice empfiehlt es sich, ein standardisiertes Incident Management Verfahren zu etablieren, das klar definiert, wie Sicherheitsvorfälle identifiziert, analysiert, gemeldet und behoben werden. Dabei sollten alle relevanten Systeme berücksichtigt und standardisierte Abläufe für Benachrichtigung, Untersuchung, Wiederherstellung sowie Nachbearbeitung festgelegt werden. Um eine effiziente und regelkonforme Bearbeitung sicherzustellen, erhalten die zuständigen Mitarbeitenden regelmässige Schulungen.

Die Verantwortung für die Überwachung der Sicherheitsrichtlinien und deren Einhaltung soll klar einer oder mehreren Personen zugewiesen werden. Diese Personen sind auch für die regelmässige Aktualisierung der Richtlinien zuständig, damit diese stets den neuesten regulatorischen Anforderungen und technologischen Entwicklungen entsprechen.

4.4.3. Praxisbeispiele

Zugriffsmanagement: Implementierung eines rollenbasierten Zugriffskontrollsystems, gemäss Kap. 4.5, das den Zugriff auf die GA-Systeme nur autorisierten Personen ermöglicht. Regelmässige Überprüfung der Zugriffsrechte, insbesondere bei Personalwechsel.

Incident Management: Einrichtung eines Incident Management Verfahrens (Vorfallreaktionsverfahren), das Schritte zur Identifizierung, Bewertung, Eindämmung und Behebung von Sicherheitsvorfällen beschreibt. Dafür sind entsprechende Schulungen des zuständigen Personals zur effektiven Anwendung des Verfahrens notwendig.

Netzwerksegmentierung: Entwicklung einer Sicherheitsrichtlinie, welche die logische Trennung von IKT-Netzwerken in der Gebäudeautomation vorschreibt, um die Auswirkungen von Angriffen zu begrenzen und kritische Systeme zu schützen. Weitere Infos sind in Kapitel 5.5 beschrieben.

4.5. Rollen und Verantwortlichkeiten

4.5.1. Sinn und Zweck

Mit der Verbindung zwischen OT und IT sind auch die Verantwortlichkeiten in den beiden Bereichen zu klären. Der KBOB Leitfaden BACnet Anwendung [2] beschreibt bereits die Rolle des BACnet Administrators und dessen Aufgaben, Kompetenzen und Verantwortungen (AKV). Mit dem Fokus IKT-Sicherheit werden hier einige weitere Rollen vorgeschlagen und ihre AKVs ausformuliert, welche sich eine Organisation bedienen kann.

Hinweis: Diese Auflistung ist nicht abschliessend und kann je nach Bedarf um zusätzliche Rollen ergänzt oder bestehende Rollen angepasst bzw. entfernt werden.

4.5.2. Best Practice Ansatz

GA-Akteure	Beschreibung
GA-Administrator ITIL: IT-Operator	**Aufgaben:** Technische Verantwortung für die GA-Infrastruktur und -Konfiguration. **Kompetenzen:** Administration und Konfiguration der GA. **Verantwortung:** Sicherstellung, dass die durch GA verwalteten Objekte und Prozesse den Betriebsanforderungen genügen (technische Verantwortung). Sicherstellung der Protokollierung und Überwachung von sicherheitskritischen Ereignissen in der GA. Da es sich bei den GA-Geräten und -Diensten um hochkritische Systemkomponenten handelt, ist diese Aufgabe mit grösster Sorgfalt auszuführen.
GA-Betrieb ITIL: Support, IT Operations Manager, IT-Operator, Major Incident Team, Problem Manager	**Aufgaben:** Verantwortlich für alle GA-Betriebsaktivitäten. **Kompetenzen:** Einführen und Betreiben der GA-Supportorganisation (First Level, Second Level, Third Level) unter Einbezug des Service Desk sowie der ICT-Betriebsorganisation. **Verantwortung:** Bereitstellen der für die Erbringung des GA-Service geeigneten Supportorganisation (First Level, Second Level, Third Level). Erstellen der Service Level Agreements unter den verschiedenen involvierten Organisationen. Implementierung und Betrieb eines Incident-Management-Prozesses speziell für GA-spezifische Herausforderungen.
GA-Führung ITIL: Compliance Manager, Availability Manager, Capacity Manager, Risikomanager	**Aufgaben:** Management (Entscheid) für Governance, Risk Management und Compliance. Entscheidet abschliessend über die GA-IKT-Vorgaben sowie über die Vorgaben für den Betrieb. Dazu gehört auch die formelle Abnahme des GA-Konzepts. Die GA-Führung ist verantwortlich für das Verwalten des GA-Services in allen Fachbereichen, wie z. B. Release-Management, Qualitätsmanagement, GA-Lieferanten- und Konsumentenmanagement, Vorfall-, Event-, Service-Request-Management. **Kompetenzen:** Abnahme von Policies und Weisungen zu GA, z. B. der GA-Service-Beschreibung, der GA-Betriebsdokumente sowie Übernahme von Restrisiken aus der Risikoanalyse. **Verantwortung:** Sicherstellung der Governance; Sicherstellung des Risikomanagements; Sicherstellung Compliance. Förderung von Schulungsprogrammen und Sicherheitskultur innerhalb der Organisation.
GA-Lieferant ITIL: Service Catalogue Manager	**Aufgaben:** Lieferung, Installation, Wartung u./o. Betrieb von Gebäudeautomation-Technik im Auftrag der Organisation. **Kompetenzen:** Beurteilung der GA der Organisation gemäss den Vorgaben des GA-Konzepts (GA-Infrastruktur, Prozesse, umgesetzte Architektur etc.). **Verantwortung:** Stellt sicher, dass die GA entsprechend den Vorgaben des GA-Konzepts aufgebaut wird. Stellt sicher, dass die GA ordnungsgemäss dem GA-Betrieb übergeben wird. Unterstützt bei der Einhaltung von Sicherheits- und Compliance-Standards während der gesamten Lebensdauer der GA.
GA-Verantwortliche/r ITIL: Service-Owner	Die GA-Verantwortlichen haben die Gesamtverantwortung über die Gebäudeautomation (auch bekannt als Service Owner Fachbereich). **Aufgaben:** Sie beraten und verifizieren die GA-Prozesse, die GA-Akteure, die GA-Informationsarchitektur sowie die technische Umsetzung. **Kompetenzen:** Sie nehmen das GA-Konzept ab. **Verantwortung:** Sie prüfen das GA-Konzept auf Vollständigkeit, Konsistenz, Nachvollziehbarkeit und Compliance gemäss den Vorgaben. Entwicklung und Pflege eines Risiko-Management-Plans für die GA.
Linienvorgesetzte/r	**Aufgabe:** Sorgen dafür, dass ihre Mitarbeitenden über die für ihre Aufgaben notwendigen Berechtigungen verfügen und die IKT-Sicherheitsvorgaben einhalten. **Kompetenz:** Sie können ihre Mitarbeitende steuern und führen, und haben die Standardkompetenzen eines Linienvorgesetzten. **Verantwortung:** Sie stellen sicher, dass ihre Mitarbeitenden die Vorgaben zur IKT-Sicherheit erfüllen. Regelmässige Überprüfung der Einhaltung von Sicherheitsstandards durch die Mitarbeitenden.
Sicherheitsbeauftragte/r SiBe	**Aufgaben:** Berät zum vorgeschlagenen IKT-Sicherheit-Konzept der GA.

GA-Akteure	Beschreibung
ITIL: Information Security Manager	**Kompetenzen:** Weisungsbefugt für die Sicherheitsaspekte der angestrebten GA-Lösung. **Verantwortung:** Sicherstellung der Identifikation, Einschätzung und Adressierung von Sicherheitsrisiken. Sicherstellung der Policy-Konformität der GA-Architektur. Prüfung der Compliance bei Funktionstrennung, Konflikten oder sensitiven Berechtigungen. Review des Berechtigungskonzepts. Sicherstellung der kontinuierlichen Schulung und Sensibilisierung aller beteiligten Akteure im Bereich GA-Sicherheit als ergänzend zur GA-Führung.
GA-Sicherheitsanalyst/in ITIL: Security Analyst	**Aufgaben:** Identifiziert Schwachstellen, bewertet Risiken und entwickelt Massnahmen zur Risikominderung. Er überwacht sicherheitskritische Ereignisse und analysiert Bedrohungen, um Sicherheitsvorfälle zu verhindern. **Kompetenzen:** Fundierte Kenntnisse in IT- und OT-Sicherheit, Bedrohungsanalyse und Schwachstellenmanagement sowie Erfahrung in der Entwicklung und Umsetzung von Sicherheitskonzepten. **Verantwortung**: Sicherstellung, dass Sicherheitslücken erkannt und geschlossen werden. Beratung der Organisation bei der Umsetzung von Sicherheitsrichtlinien und -massnahmen.
GA-Architekt/in ITIL: IT Architect	**Aufgaben:** Plant und entwirft die GA-Architektur, stellt deren Skalierbarkeit und Integration sicher und bewertet kontinuierlich neue Technologien für die Optimierung der Infrastruktur. **Kompetenzen:** Expertise in Systemarchitektur, Netzwerken und Sicherheitsstandards sowie Erfahrung in der Integration von IT- und OT-Systemen. **Verantwortung:** Gewährleisten, dass die Architektur den aktuellen und zukünftigen Anforderungen entspricht und nachhaltige Lösungen entwickeln, die mit den strategischen Zielen der Organisation harmonieren.
GA-Trainer/ Schulungsbeauftragte/r ITIL: Knowledge Manager	**Aufgaben:** Sicherstellen, dass alle relevanten Beteiligten die notwendigen Kenntnisse für ihre Aufgaben haben, insbesondere in den Bereichen Sicherheit und Compliance. Planung, Durchführung und Nachverfolgung von Schulungen für die GA-Systeme und -Prozesse. **Kompetenzen:** Erstellung und Vermittlung von zielgerichteten Schulungsinhalten für GA. Kenntnisse in Sicherheits- und Compliance-Anforderungen. Fähigkeit, Trainingsprogramme effizient zu planen und durchzuführen. **Verantwortung:** Sicherstellen, dass alle Beteiligten über ausreichendes Wissen verfügen, um die Betriebssicherheit und Compliance der GA zu gewährleisten. Förderung von Sicherheits- und Lernkultur innerhalb der Organisation.
Auditor/in Revisor/in	**Aufgaben:** Führt Audits bzw. Revisionen durch, z. B. bezüglich der Umsetzung der GA-Architektur und des Betriebs der GA. **Kompetenzen:** Festlegung, was wann und wie auditiert wird. **Verantwortung:** Durchführung von Audits gemäss der festgelegten Audit Policy der Organisation. Involvierte Organisationen: Extern oder von einer anderen internen Stelle (Gewaltentrennung) als die GA-Administratoren.

Tabelle 1: Rollen und Verantwortlichkeiten für IKT-Sicherheit der GA

4.5.3. Praxisbeispiel

Um die Überführung der Gebäudeautomation in den Betrieb sicherzustellen und die definierten Rollen optimal zu implementieren, ist ein systematischer Ansatz erforderlich.

Definition eines strukturierten Übergabeprozesses an den Betrieb

Nach erfolgreicher Durchführung der Abnahmetests, bei denen die Funktionalität der neuen oder angepassten Gebäudeautomationssysteme unter realistischen Bedingungen überprüft wurde, erfolgt die Übergabe der Systeme von den GA-Lieferanten an den GA-Betrieb. Dieser Übergabeprozess wird in einem formellen Protokoll dokumentiert, das von den beteiligten Akteuren – den GA-Lieferanten und dem Vertreter des GA-Betriebs – unterzeichnet wird. Dabei werden alle relevanten Dokumentationen wie technische Spezifikationen, Konfigurationshandbücher und Testprotokolle beigelegt.

Im Anschluss organisiert der GA-Trainer eine der Anlagengrösse entsprechende Schulung für die GA-Administratoren und das GA-Betriebsteam. In dieser Schulung werden sowohl die Bedienung als auch die Konfiguration des neuen Systems detailliert vermittelt. Dabei liegt der Fokus auf praxisnahen Übungen, z. B. dem Umgang mit Alarmszenarien und der Konfiguration von Zugriffsrechten.

Zur Qualitätssicherung führt der Sicherheitsbeauftragte wenige Tage nach der Übergabe ein umfassendes Audit durch (Kapitel 4.11). Ziel des Audits ist es, die Einhaltung der Sicherheitsvorgaben, wie z. B. die korrekte Umsetzung von Funktionstrennungen und die Einhaltung der Zugriffsrichtlinien, zu überprüfen. Etwaige Abweichungen werden dokumentiert und dem GA-Betrieb zur Nachbesserung gemeldet.

Parallel dazu richtet der GA-Administrator ein umfassendes Überwachungssystem ein (Kapitel 4.9). Dieses System protokolliert sicherheitskritische Ereignisse, wie z.B. unautorisierte Zugriffsversuche oder ungewöhnliche Netzwerkaktivitäten, in Echtzeit und stellt diese Informationen in einem Dashboard zur Analyse bereit. So wird sichergestellt, dass potenzielle Sicherheitsrisiken frühzeitig erkannt und entsprechend adressiert werden können.

4.6. Schulung und Bewusstsein

4.6.1. Sinn und Zweck

Ein bekanntes Mantra der Informationssicherheit ist «der Mensch ist das schwächste Glied der Kette». Dies ist jedoch nicht als Schuldzuweisung auf Mitarbeitenden zu verstehen, sondern stattdessen als Erinnerung daran, wie wichtig Sicherheitsbewusstsein und Schulung der Mitarbeitenden für Sicherheit einer Organisation sind.

Mitarbeitende, die ihre Rollen und Verantwortlichkeiten in der Informationssicherheit verstehen und leben, ein Auge offen haben für mögliche Sicherheitsvorfälle sowie gute IT-Hygiene pflegen, sind ein Bollwerk für jedes Sicherheitsprogramm. Oft können sie besser als jedes Sicherheitstool Anomalien erkennen und mit ihrem Fachwissen ein wichtiger Bestandteil der Reaktion auf etwaige Vorfälle sein. Vor allem im OT-Umfeld ist dies oft schon eingespielt mit sogenannten «Safety» Schulungen und Kampagnen. Hier bietet es sich an, die Informationssicherheit als nichts neues und separates, sondern als eine Ergänzung der bisherigen Sicherheitsschulungen und «Awareness»-Kampagnen zu behandeln. Denn ob z. B. die Lüftung eines Rechenzentrums aufgrund eines Hardware-Defekts oder einer Cyber Attacke ausfällt, macht keinen Unterschied für die Mitarbeitenden, deren Sicherheit ist so oder so davon betroffen.

Sicherheitsbewusstsein und Schulungen lassen sich dementsprechend auch in sämtlichen gängigen Frameworks und Standards der Informationssicherheit verorten. Der NIST CSF [3] empfiehlt im Bereich «Protect» die «Sensibilisierung und Ausbildung» der Mitarbeitenden und externen Partner. Der IT-fokussierte ISO-27001-2022 Standard [8] kennt als organisatorische Massnahme die Kontrolle «6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung» als essenzieller Teil eines jeden ISMS. Der OT-fokussierte ISA/IEC-62443-2-1 Standard [4] kennt ebenso die Schulung und Sicherheitsbewusstsein als essenzieller Teil eines jeden CSMS, welches das OT-Gegenstück zum ISMS ist.

Die Schulung gilt dabei nicht nur für die regulären Mitarbeitenden, sondern auch für Personen in der Sicherheitsorganisation oder mit Sicherheitsverantwortlichkeiten, damit diese über ihre Aufgaben informiert und für diese vorbereitet werden.

4.6.2. Best Practice Ansatz

Ein strukturiertes Schulungs- und Sicherheitsbewusstseinsprogramm versucht bewusst, die Mitarbeitenden in ihrem Arbeitsalltag zu begleiten. Bereits beim Arbeitsbeginn sollten Mitarbeitende eine gezielte Sicherheitsschulung durchlaufen, um ein solides Grundverständnis der relevanten Bedrohungen in der Informationssicherheit zu entwickeln und notwendige Sicherheitsrichtlinien und -weisungen kennenzulernen. Regelmässige «Auffrisch»-Kurse stellen sicher, dass das Bewusstsein und das Sachverständnis der Mitarbeitenden aktuell bleiben. Hierbei empfiehlt sich, die theoretischen Schulungen durch praxisnahe Angebote zu ergänzen, welche sowohl das Gelernte vertiefen als auch die Mitarbeitenden für den Umgang mit Informationssicherheit sensibilisieren. Ein beliebtes Format ist eine sog. «Security Roadshow», wo Mitarbeitenden häufige Sicherheitsvorfälle gezeigt werden, teilweise interaktiv. Als mögliche Beispiele sind die Nutzung von sog. «Rubber Ducky» USB-Sticks, die Simulation von Ransomware-Angriffen oder die Demonstration der Detektion von Sicherheitsvorfällen.

Zudem können Schulungen durch interne Kommunikationsmittel wie E-Mails, Poster und interaktive Kampagnen unterstützt werden, die Sicherheitsaspekte und aktuelle Bedrohungslagen regelmässig ins Gedächtnis rufen. Ein etabliertes Phishing-Simulationsprogramm mit begleitendem Informationsmaterial bietet darüber hinaus eine praxisnahe Möglichkeit, Wissen zu testen und das Bewusstsein für Bedrohungen weiter zu schärfen.

Ein weiterer zentraler Baustein ist die Förderung einer offenen Sicherheitskultur, in der Vorfälle gemeldet und gemeinsam bearbeitet werden können. Hiermit wird durch die Vermeidung von Schuldzuweisungen eine «Angstkultur» verhindert, welche nicht nur das Vertrauen schwächen kann, sondern auch dazu führt, dass Fehler oder Bedrohungen aus Angst vor Konsequenzen verschwiegen werden. In diesem Sinne sollte es für Mitarbeitende auch klar erkennbare Ansprechpartner geben, denen sie auch vermeintliche triviale Fragen zur Informationssicherheit stellen können. Mitarbeitende sind oft die ersten, die Anomalien oder mögliche Bedrohungen wahrnehmen. Ihr Feedback kann eine wichtige Quelle für frühzeitige Bedrohungserkennung sein.

4.6.3. Praxisbeispiel

Wie in Kapitel 4.7 beschrieben, ist ein guter Notfallplan eine essenzielle Vorsorge gegen Vorfälle jeglicher Art, inklusive Cybersecurity-Vorfälle. Allerdings sind derartige Pläne nur wirksam, wenn sie auch regelmässig geschult und geübt werden. Hierbei kann eine sogenannte «Tabletop-Exercise» ein gutes Praxisbeispiel sein, wie man effektiv Krisenbewältigung übt, Wissenslücken und -unklarheiten aufdeckt und ein erhöhtes Sicherheitsbewusstsein schafft.

In einer «Tabletop-Exercise» [9] wird den Teilnehmenden ein konkreter und realistischer fiktiver Sicherheitsvorfall vorgestellt und dann der dazugehörige Notfallplan an einem

Tisch mit Hilfsmaterial wie Spielfiguren und Notizzettel durchgespielt. Hierbei ist es wichtig, eine repräsentative Mischung von Mitarbeitenden zu involvieren, vom Führungsteam über Sicherheitspersonal zu Angestellten im Betrieb, und diesen den Freiraum gegeben wird, in dieser Simulation auch Fehler machen zu dürfen. Deswegen ist es wichtig, bei der Durchführung wichtige Entscheidungen und Gesprächspunkte zu sammeln, um dann abschliessend in der Gruppe ein sogenanntes «Debriefing» durchzuführen. Hier wird rekapituliert, was gut funktioniert hat, was unklar war und wo es konkretes Verbesserungspotenzial gibt. Solange dies ohne Schuldzuweisung und mit konstruktivem Feedback erfolgt, ist diese «Tabletop-Exercise» eine sehr effektive und praktische Lernerfahrungen für die Mitarbeitenden. Sie ist gleichzeitig auch verträglicher für den Betrieb als ein «echter» Notfalltest.

4.7. Risikomanagement und Notfallplanung

In der OT ist ein effektives Risikomanagement keine Option, sondern eine strategische Notwendigkeit. Durch die zunehmende Vernetzung industrieller Systeme steigt die Angriffsfläche – und damit auch die potenzielle Bedrohung für die Produktion, Sicherheit und Unternehmensreputation. Ohne eine fundierte Notfallplanung können bereits kleinste Vorfälle schwerwiegende Folgen haben. Deshalb ist es entscheidend, Risiken frühzeitig zu identifizieren, zu bewerten und durch gezielte Massnahmen abzusichern. Nur so lassen sich Ausfälle minimieren, Reaktionszeiten optimieren und die Resilienz der OT-Landschaft nachhaltig stärken.

Angesichts dieser zentralen Rolle kommt diesem Thema in der vorliegenden Strategie eine besondere Bedeutung zu. Das folgende Kapitel widmet sich daher ausführlich den Anforderungen, Prinzipien und Massnahmen eines ganzheitlichen OT-Risikomanagements und einer praxistauglichen Notfallplanung – unverzichtbare Säulen für den sicheren und zuverlässigen Betrieb.

4.7.1. Sinn und Zweck

Im Bereich der IT- und OT-Technologien spielen Risikomanagement und Notfallmanagement eine zentrale Rolle, um die Sicherheit und Resilienz kritischer Systeme zu gewährleisten. IT-Systeme umfassen Netzwerke, Datenbanken und Anwendungen, die Unternehmensinformationen verarbeiten, während OT-Systeme für die Steuerung und Überwachung von physischen Prozessen verantwortlich sind (z. B. in Produktionsanlagen oder Energieversorgungsnetzen). Durch die zunehmende Vernetzung dieser Systeme, insbesondere im Kontext von Industrie 4.0, werden Sicherheitsanforderungen immer wichtiger, um Cyberangriffe und Betriebsunterbrechungen zu verhindern. Die Normen NIST CSF 2.0 und ISA/IEC-62443 bieten umfassende Rahmenwerke und Leitlinien, um Sicherheitsrisiken zu identifizieren, zu bewerten und zu managen.

Im Risikomanagement geht es darum, Sicherheitsrisiken zu identifizieren, zu bewerten und geeignete Massnahmen zur Risikominderung zu implementieren. Gemäss NIST CSF [3] gehört Risikomanagement zu den Kategorien «Identify», «Detect» und «Protect». Der Zweck besteht darin, potenzielle Bedrohungen für IT- und OT-Systeme zu erkennen und sicherzustellen, dass geeignete Massnahmen ergriffen werden, um den Betrieb vor negativen Einflüssen zu schützen. Das umfasst die Bewertung von Schwachstellen, potenziellen Bedrohungen wie Cyberangriffen, Systemausfällen oder menschlichem Versagen und den Folgen, die für den Betrieb ein Risiko darstellen.

Das Notfallmanagement zielt darauf ab, schnell auf Vorfälle zu reagieren, um Ausfallzeiten zu minimieren und den normalen Betrieb wiederherzustellen. Der Hauptzweck besteht darin, eine gut vorbereitete Reaktion auf Notfälle wie Cyberangriffe, Systemausfälle

oder physische Katastrophen zu gewährleisten, damit Auswirkungen auf IT- und OT-Systeme begrenzt bleiben.

Der ISA/IEC-62443 Standard ermöglicht es Unternehmen, Sicherheitslücken und Bedrohungen zu identifizieren und mithilfe eines strukturierten Ansatzes Risiken zu minimieren. ISA/IEC-62443 konzentriert sich ebenfalls auf die Absicherung von Steuerungssystemen und die Wiederherstellung der Produktion nach Vorfällen. Dabei werden technische und organisatorische Massnahmen beschrieben, die sowohl den Betrieb als auch die Sicherheit aufrechterhalten sollen. Hierzu gehört auch die Erstellung und Pflege von Wiederherstellungsplänen für kritische Infrastrukturen, die die Auswirkungen eines Ausfalls minimieren. Die NIST CSF 2.0 bietet ebenfalls klare Richtlinien zur Erstellung eines Notfallmanagementplans. Im Rahmen der «Respond»- und «Recover»-Funktionen werden Unternehmen ermutigt, geeignete Pläne zur Schadensbegrenzung und Wiederherstellung zu entwickeln.

Risikomanagement und Notfallmanagement sind essenziell, um die Sicherheit und den kontinuierlichen Betrieb von IT- und OT-Systemen zu gewährleisten. Sie bieten einen strukturierten Ansatz zur Identifizierung von Risiken, zum Schutz vor Bedrohungen und zur schnellen Wiederherstellung nach Vorfällen. Durch die Implementierung von Standards können Unternehmen eine robuste Sicherheitsstrategie entwickeln, die auf die spezifischen Anforderungen von IT- und OT-Technologien zugeschnitten ist.

4.7.2. Best Practice Ansatz

Ein effektives Risiko- und Notfallmanagement erfordert die Zusammenarbeit zwischen technischen Experten, dem Management und Schulungsteams. Ein formaler Prozess zur kontinuierlichen Risikobewertung und -minderung sollte implementiert werden. Sicherheitszonen und Netzwerksegmentierung isolieren potenzielle Bedrohungen, wobei unterschiedliche Sicherheitsstufen je nach Risiko für Systeme und Zonen angewandt werden, um ein angemessenes Schutzniveau zu gewährleisten. Sicherheitsaspekte sollten über den gesamten Lebenszyklus von Produkten und Systemen hinweg berücksichtigt werden, von der Entwicklung bis zur Ausserbetriebnahme.

Rollen im Risikomanagement
Wichtige Rollen sind IKT-Sicherheitsbeauftragte, Ingenieure und IKT-Notfallmanager, die potenzielle Bedrohungen analysieren. IKT-Risikomanager und Business-Continuity-Manager koordinieren Strategien zur Risikominderung und Wiederherstellung. CISOs und Compliance-Manager sorgen dafür, dass alle Massnahmen den gesetzlichen Vorschriften entsprechen. Schulungen und Sensibilisierung der Mitarbeitenden sind von entscheidender Bedeutung, wobei regelmässige Übungen die Vertrautheit mit Best Practices im Risiko- und Notfallmanagement fördern und eine Sicherheitskultur im Unternehmen etablieren.

Umfassende Notfallplanung
Um eine effektive Reaktion auf Vorfälle zu gewährleisten, müssen umfassende Notfallpläne erstellt werden. Dazu gehören ein Desaster-Recovery-Plan (DRP) zur Wiederherstellung von OT-Systemen nach einem Vorfall und ein Business-Continuity-Plan (BCP), um den Betrieb während und nach einem Vorfall aufrechtzuerhalten sowie ein Incident Response Plan (IRP), der klare Schritte und Verantwortlichkeiten für die Identifikation, Eindämmung, Behebung und Nachbearbeitung von Sicherheitsvorfällen definiert. Ein Kommunikationsplan sollte entwickelt werden, um während eines Vorfalls klare und effiziente Kommunikationswege zu gewährleisten.

Tests und Koordination
Regelmässige Tests der Notfallpläne sind notwendig, um sicherzustellen, dass alle

Beteiligten im Ernstfall handlungsfähig sind. Die Abstimmung mit Dienstleistern ist ebenfalls entscheidend, damit deren Notfallpläne mit den eigenen übereinstimmen.

Regelmässige Schulungen und Simulationen
Schulungen der Mitarbeitenden in Notfallverfahren sind entscheidend, um sicherzustellen, dass alle relevanten Personen auf Notfälle vorbereitet sind. Regelmässige Übungen und Simulationen sollten durchgeführt werden, um die Wirksamkeit der Notfallpläne zu testen. Überwachungssysteme müssen implementiert werden, um ungewöhnliche Aktivitäten und potenzielle Bedrohungen frühzeitig zu erkennen. Ein Incident-Response-Team sollte bereitstehen, um bei Sicherheitsvorfällen schnell und effektiv reagieren zu können.

Wiederherstellung und Analyse nach Vorfällen
Die Wiederherstellung und der Wiederaufbau von OT-Systemen nach einem Vorfall müssen durch klar definierte Prozesse geregelt sein, die regelmässig auf ihre Wirksamkeit getestet werden. Nach jedem Vorfall sollte eine gründliche Analyse durchgeführt werden, um festzustellen, was gut funktioniert hat und wo Verbesserungen notwendig sind. Diese Erkenntnisse sollten genutzt werden, um die Notfallpläne kontinuierlich zu aktualisieren und weiterzuentwickeln, um auf Veränderungen in der Bedrohungslandschaft vorbereitet zu sein.

4.7.3. Checkliste für Risikomanagement und Notfallplanung

Eine Checkliste ist für das IKT- und OT-Risikomanagement äusserst hilfreich, da sie sicherstellt, dass alle wichtigen Schritte systematisch und vollständig abgearbeitet werden. Sie hilft dabei, nichts zu übersehen, insbesondere in komplexen Notfall- und Risikomanagementprozessen, wo es entscheidend ist, dass alle Beteiligten ihre Aufgaben klar kennen. Durch eine Checkliste können Verantwortlichkeiten klar verteilt, der Ablauf von Notfallplänen effizienter gestaltet und regelmässige Überprüfungen und Tests strukturiert durchgeführt werden. Zudem trägt sie zur Standardisierung von Prozessen bei und vereinfacht die Kommunikation und Koordination zwischen verschiedenen Teams und Dienstleistern.

Empfehlung	Beschreibung
Risikobewertung und -management	Systematische Identifizierung und Bewertung von Risiken
Sicherheitszonen und Segmentierung	Aufteilung des Netzwerks in Sicherheitszonen und Segmentierung
Sicherheitsstufen anwenden	Definieren und Umsetzen der passenden Sicherheitsstufen
Sicherheitslebenszyklus verwalten	Implementierung von Sicherheitsmassnahmen über den gesamten Produktlebenszyklus
Notfallpläne testen	Regelmässige Tests von Notfallplänen zur Gewährleistung der Wirksamkeit
Koordination mit Dienstleistern	Abstimmung von Notfallplänen mit externen Dienstleistern
Redundanz und Backups implementieren	Sicherstellung von Backup-Systemen und redundanter Infrastruktur
Manuelle Steuerung ermöglichen	Manuelle Steuerung kritischer Systeme im Notfall ermöglichen
Regelmässige Überprüfung der Systeme	Kontinuierliche Überprüfung der Sicherheitsmechanismen und -protokolle
Wiederherstellungspläne definieren	Definieren von Massnahmen zur schnellen Wiederherstellung im Falle eines Vorfalls

Tabelle 2: Checkliste für Risikomanagement und Notfallplanung

Schritt	Beschreibung
Erkennung Detection	Der Sicherheitsvorfall wird durch Monitoring-Systeme, Benachrichtigungen oder Meldungen identifiziert. Das Incident Response Team bewertet die Situation und bestimmt die Kritikalität des Vorfalls.
Reaktion Detection	Sofortige Reaktion zur Eindämmung des Vorfalls, z. B. durch Trennen betroffener Systeme vom Netzwerk. Relevante Beweise (Logdateien, Systembilder) werden gesichert, um weitere Analysen zu ermöglichen.
Eindämmung Mitigation	Massnahmen zur Begrenzung des Schadensumfangs, z. B. durch Entfernen schädlicher Software, Blockieren verdächtiger IP-Adressen oder Beheben von Schwachstellen, die den Vorfall verursacht haben.
Berichterstattung Reporting	Sorgfältige Dokumentation des gesamten Vorfalls, einschliesslich aller Reaktionen und Massnahmen. Erstellung detaillierter Berichte für interne Stakeholder und externe Behörden, falls erforderlich.
Wiederherstellung Recovery	Gezielte Wiederherstellung der betroffenen Systeme, einschliesslich Einspielen sauberer Backups, Neuinstallation von Software oder Rücksetzen von Konfigurationen. Sicherstellung eines stabilen Betriebs.
Abhilfemassnahmen Remediation	Implementierung dauerhafter Massnahmen, um ähnliche Vorfälle zu verhindern, wie z. B. Installation von Sicherheitsupdates, Verbesserung von Zugriffskontrollen oder Anpassung von Sicherheitsrichtlinien.
Lernerfahrung Lessons Learned	Durchführung einer gründlichen Nachanalyse, um aus dem Vorfall zu lernen. Identifikation von Schwachstellen im Prozess und Implementierung von Verbesserungen für eine effektivere Reaktion in der Zukunft.

Tabelle 3: Empfehlung Aufbau Incident Response Plan

4.7.4. Praxisbeispiel

Als Praxisbeispiel wurde 2023 eine kritische Zero-Day-Schwachstelle in MOVEit Transfer, einer weit verbreiteten Software für Dateiübertragungen, entdeckt. Diese Schwachstelle ermöglichte es Angreifern, unbefugten Zugriff auf sensible Daten von zahlreichen Organisationen zu erlangen, die diese Software nutzten. MOVEit Transfer wird von vielen Unternehmen und Regierungsbehörden eingesetzt, um sichere Dateiübertragungen durchzuführen, was die Software zu einem attraktiven Ziel für Cyberkriminelle machte.

Angreifer nutzten diese Schwachstelle, um grosse Mengen an Daten zu stehlen, darunter persönliche, finanzielle und vertrauliche Geschäftsinformationen. Der Vorfall betraf eine Vielzahl von Branchen, einschliesslich des Gesundheitswesens, der Finanzindustrie und des öffentlichen Sektors. Einige Organisationen erlitten erhebliche finanzielle Verluste, standen unter regulatorischer Beobachtung und mussten mit einem Reputationsschaden kämpfen, da sensible Informationen offengelegt wurden.

Organisationen mit einer soliden Risikomanagement-Strategie hatten bereits Dateiübertragungssysteme wie MOVEit als kritische Bestandteile ihrer IT-Infrastruktur identifiziert. Durch regelmässige Sicherheitsbewertungen und Schwachstellenscans waren diese Organisationen sich potenzieller Bedrohungen bewusst und besser darauf vorbereitet, sie zu mindern. Einige hatten sogar Risiko-Behandlungsstrategien (z. B. basiert auf ISO 27001 und dem NIST CSF 2.0) implementiert, wie die Verschlüsselung von Daten, die Segmentierung sensibler Systeme und mehrschichtige Sicherheitsmassnahmen, um den möglichen Schaden im Falle einer Ausnutzung der Schwachstelle zu minimieren.

Die Incident-Response-Pläne dieser Organisationen spielten eine entscheidende Rolle. Sie hatten festgelegte Verfahren zur Reaktion auf Datenverstösse oder Systemschwachstellen, die es ihnen ermöglichten, kompromittierte Systeme zu isolieren, betroffene Stakeholder schnell und transparent zu informieren, mit Anbietern und Sicherheitsteams zusammenzuarbeiten und forensische Untersuchungen durchzuführen. Organisationen mit robusten Desaster-Recovery-Plänen konnten betroffene Dienste schneller wiederherstellen und Ausfallzeiten minimieren. Durch vordefinierte Rollen und Verantwortlichkeiten, Kommunikationsprotokolle und Wiederherstellungsschritte konnten sie die Krise effektiv bewältigen, ohne weitreichende Störungen ihrer Abläufe zu verursachen.

Nachdem die unmittelbare Krise bewältigt war, führten die betroffenen Unternehmen Nachuntersuchungen des Vorfalls durch, um Lücken in ihren Reaktionsstrategien zu identifizieren und ihr Sicherheitsframework zu verbessern. Die aus dem MOVEit-Vorfall gewonnenen Erkenntnisse ermutigen Organisationen, ihre Anbieter-Management-Praktiken weiter zu stärken, kontinuierliche Überwachung von Drittanbieteranwendungen einzuführen und ihre Incident-Response-Fähigkeiten zu verbessern.

Der MOVEit-Vorfall dient als herausragendes Beispiel dafür, wie entscheidend proaktives Risikomanagement und gut geplante Incident-Response-Massnahmen sind, um die Auswirkungen von Cyberangriffen zu mildern. Organisationen, die diese Praktiken in ihre Sicherheitsframeworks integriert hatten, konnten nicht nur den Schaden begrenzen, sondern auch schneller wiederherstellen und zeigten eine hohe Resilienz gegenüber Cyberbedrohungen. Der Vorfall unterstreicht die zunehmende Bedeutung der Sicherung von Drittanbieter-Software und die Notwendigkeit kontinuierlicher Wachsamkeit angesichts des sich ständig weiterentwickelnden Bedrohungsumfelds.

4.8. Asset- und Lifecycle Management

4.8.1. Sinn und Zweck

Asset- und Lifecycle-Management sind entscheidende Komponenten zur Sicherstellung der OT-Sicherheit in modernen Unternehmen. Diese Strategien bieten eine systematische Herangehensweise zur Verwaltung und Sicherung der physischen und digitalen Ressourcen, die für den Betrieb unerlässlich sind. Durch ein effektives Asset-Management wird ein umfassender Überblick über alle OT-Komponenten, ihre Versionen und Konfigurationen ermöglicht. Dies hilft, potenzielle Schwachstellen zu identifizieren und gezielte Massnahmen zur Risikominderung zu ergreifen. Lifecycle-Management hingegen gewährleistet, dass Systeme und Geräte regelmässig aktualisiert und gewartet werden, um den neuesten Sicherheitsstandards zu entsprechen. Gemeinsam verbessern sie die Übersicht und Kontrolle über die OT-Infrastruktur, minimieren ungeplante Ausfallzeiten und reduzieren das Risiko von Sicherheitsvorfällen erheblich.

4.8.2. Best Practice Ansatz

Ein effektives Asset- und Lifecycle-Management ermöglicht es, alle physischen und digitalen Ressourcen eines Unternehmens zu überwachen und optimal zu nutzen. Die folgenden Best Practices helfen, die Transparenz zu erhöhen, Risiken zu minimieren und sicherzustellen, dass Systeme und Geräte während ihres gesamten Lebenszyklus sicher und effizient betrieben werden.

Eine gründliche Inventarisierung und Dokumentation von OT-Assets ist der erste Schritt zu einer effektiven Sicherheitsstrategie. Dazu gehört das Erstellen und regelmässige Aktualisieren eines umfassenden Inventars aller relevanten Hardware, Software, Firmware, Netzwerkinfrastrukturen und IoT-Geräte. Eine Kritikalitätsbewertung hilft dabei, die Assets nach ihrer Bedeutung für den Betrieb zu priorisieren und gezielte Sicherheitsmassnahmen zu planen. Gleichzeitig müssen diese Assets kontinuierlich überwacht werden, um ihren Zustand und ihre Leistung in Echtzeit zu bewerten und Anomalien oder Ausfälle frühzeitig zu erkennen. Regelmässige Inspektionen und digitale Audits stellen sicher, dass alle Assets den Sicherheitsstandards entsprechen und keine unbefugten Änderungen vorgenommen wurden. Zudem ist eine Schwachstellenbewertung erforderlich, um potenzielle Risiken, die durch veraltete Softwareversionen oder unsichere Konfigurationen entstehen könnten, rechtzeitig zu identifizieren und zu beheben.

Die Lifecycle-Management von OT-Assets umfasst alle Phasen von der Anschaffung über die Nutzung bis hin zum Rückbau und zur Entsorgung. Bereits bei der Auswahl sollten Sicherheits- und Kompatibilitätsanforderungen berücksichtigt werden. Der Rückbau erfordert eine frühzeitige Planung, insbesondere bei End-of-Life-Ankündigungen, um nahtlose Übergänge zu neuen Systemen zu ermöglichen. Bei der Entsorgung müssen sensible Daten sicher gelöscht und Geräte gemäss Umwelt- und Sicherheitsstandards recycelt oder entsorgt werden. Durch klare Prozesse und Verantwortlichkeiten entlang des gesamten Lebenszyklus können Risiken minimiert, die Betriebssicherheit erhöht und gesetzliche sowie umweltbezogene Anforderungen erfüllt werden.

Ein effektives Patch-Management ist entscheidend für die OT-Sicherheit (Kapitel 4.10). Es umfasst die regelmässige Überprüfung und Anwendung von verfügbaren Sicherheitspatches und Updates, um bekannte Schwachstellen zu beheben und Systeme gegen neue Bedrohungen zu schützen. Patches sollten zunächst in einer Testumgebung geprüft werden, um die Systemstabilität zu gewährleisten, bevor sie in der Produktionsumgebung implementiert werden. Hierbei ist auch die Lieferantenbeziehung zu berücksichtigen, insbesondere das «Patching» mit Einverständnis des Herstellers passiert, um hiermit nicht ungewollt die Garantie des Produktes nichtig zu machen.

Eng verknüpft damit ist das Change Management, das einen strukturierten Änderungsprozess für OT-Assets sicherstellt. Dies beinhaltet die Prüfung, Genehmigung und Dokumentation aller Änderungen sowie die Bewertung potenzieller Risiken und die Vorbereitung von Rollback-Plänen, falls Änderungen unerwartete Probleme verursachen.

Beim End-of-Life-Management geht es darum, den Lebenszyklusstatus aller OT-Assets zu überwachen, um rechtzeitig den Austausch veralteter oder nicht mehr unterstützter Geräte und Software zu planen. Dabei ist es wichtig, Daten sicher zu entfernen und zu löschen, um zu verhindern, dass sensible Informationen kompromittiert werden.

Die Schulung und Sensibilisierung von Mitarbeitenden sind zentrale Elemente eines wirksamen Asset- und Lifecycle-Managements in der OT-Sicherheit. Regelmässige Schulungen stellen sicher, dass alle Mitarbeitenden, die mit OT-Systemen arbeiten, die Prinzipien des Asset- und Lifecycle-Managements verstehen und korrekt anwenden können. Awareness-Programme betonen die Bedeutung der Sicherheit und fördern beständige Sicherheitspraktiken im OT-Bereich. Ergänzend dazu sollte eine kontinuierliche Verbesserung der Prozesse angestrebt werden. Dies umfasst regelmässige Überprüfungen und Aktualisierungen der Asset- und Lifecycle-Management-Prozesse, die auf neuen Bedrohungen, technologischen Entwicklungen und den Erfahrungen aus Vorfällen basieren. Die umfassende Dokumentation aller Prozesse, Änderungen und Ereignisse sorgt für Transparenz und unterstützt bei Audits sowie der Untersuchung von Vorfällen.

4.8.3. Checkliste für Asset- und Lifecycle-Management

Durch die Umsetzung einer Checkliste wird ein strukturierter Ansatz zur Sicherung und Verwaltung von OT-Assets über den gesamten Lebenszyklus gewährleistet.

- ✓ **Inventarisierung und Kategorisierung**
  - Vollständige Liste aller OT-Assets (Hardware, Software, Netzwerke) erstellen.
  - Assets nach Kritikalität und betrieblicher Bedeutung kategorisieren.
  - Inventar regelmässig aktualisieren und dokumentieren.
- ✓ **Lebenszyklusüberwachung**
  - Anschaffung und Implementierung: Sicherheits- und Kompatibilitätsanforderungen definieren; Hersteller- und Supportbedingungen prüfen.
  - Nutzung und Wartung: Regelmässige Wartung, Schwachstellenanalysen und Updates einplanen; Einhaltung von Sicherheitsrichtlinien sicherstellen.
  - Rückbau und Übergangsplanung: End-of-Life-Daten überwachen; Migrationspläne entwickeln und Verantwortlichkeiten klären.
  - Sichere Entsorgung: Daten sicher löschen; sichere Transport- und Entsorgungsprozesse umsetzen.
  - Recycling: Umweltstandards und gesetzliche Vorgaben beachten; zertifizierte Recyclingpartner einbinden.
- ✓ **Regelmässige Sicherheitsüberprüfungen**
  - Schwachstellenscans und Konfigurationskontrollen durchführen.
  - Patch-Management-Überprüfungen sicherstellen.
- ✓ **Rollenbasierte Verantwortlichkeiten**
  - Verantwortlichkeiten für Inventarisierung, Wartung und Stilllegung klar definieren.
  - Asset-Management-Aufgaben schriftlich festlegen und überwachen.
- ✓ **Sensibilisierung und Schulung**
  - Mitarbeiter in Best Practices für Asset- und Lebenszyklusmanagement schulen.

– Verantwortliche für OT-Sicherheitsprozesse regelmässig weiterbilden.

4.9. Überwachung und Reaktion

4.9.1. Sinn und Zweck von Überwachung und Reaktion

Kontinuierliche Überwachung und Auswertung sind entscheidend, um die Sicherheit des Netzwerks zu gewährleisten, Vorfälle zu identifizieren und auf diese reagieren, sowie die Nachvollziehbarkeit und Auditierbarkeit der Sicherheitsmassnahmen sicherzustellen. Dabei ist entscheidend, dass die blosse Datenerhebung in potenziell riesigen Volumen nicht für einen Gewinn an Sicherheit sorgt, sondern dass dies erst durch die Auswertung der Daten und die Reaktion auf identifizierte Anomalien und Vorfälle passiert. Dementsprechend ist die Quantität und Qualität der Überwachung und dementsprechend Datenerhebung den technologischen und insbesondere organisatorischen Fähigkeiten der Organisation anzupassen. Falls eine Ausweitung der Datenerhebung gewünscht ist, muss diese zwingend auch die Analysefähigkeiten der Organisation verstärken. Wichtig ist, dass technische Analysefähigkeit auch die Fähigkeit des Netzwerkes inkludiert, welches die Datenmengen transportieren muss. Insbesondere in einem OT-Umfeld wäre es z. B. fatal, wenn die Datenübertragung der Systemüberwachung diese Netze überlastet und damit selbst Ausfälle generiert.

Nach Aufbau einer zielgerichteten Überwachungs- und Analyse-Infrastruktur gilt es dann, eine sog. «Baseline» für die Netzwerk-, System- und Applikationsaktivitäten zu identifizieren. Dies erfolgt je nach Analyseansatz durch Maschinelles Lernen (ML) oder durch die Konsolidierung der Erfahrungswerte der Mitarbeitenden. Daraufhin kann das Überwachungssystem nun Anomalie oder Abweichungen erkennen und ausweisen. Sobald ein Vorfall erkannt und lokalisiert ist, wird eine zeitnahe Reaktion durch sog. «Runbooks» realisiert. Diese sind «Vorfallspläne», analog zu den bekannteren «Notfallplänen», welche im Voraus definiert sind, wie auf verschiedene Informationssicherheitsvorfälle zu reagieren ist. Dies erlaubt ungewollte Nebenwirkungen von Massnahmen zu vermeiden, klärt im Voraus die Prioritäten von verschiedenen Systemen ab und erlaubt im Vorfallszenario eine zielgerichtete und koordinierte Reaktion.

Die kontinuierliche Überwachung und deren Dokumentation durch verschiedene Log-Dateien hat aber auch eine wichtige Rolle für Audits und für die digitale Forensik nach Vorfällen. Im ersten Fall gewährleistet die Überwachung die Nachvollziehbarkeit von «wer hat was wann wo gemacht», welches für Audits wichtig ist. Wenn z. B. eine Kälteanlage ausserplanmässig ausgeschaltet wird, kann man so nachvollziehen, welcher Steuerungsvorgang dies ausgelöst hat. Die kontinuierliche Überwachung unterstützt aber auch während und nach Cybersecurity-Vorfällen, da hieraus der Tatenverlauf der Angreifer identifiziert werden kann. Dies ist essenziell, um erneute Vorfälle gleicher Art zu verhindern. So kann z. B. identifiziert werden, dass der Ausgangspunkt des Angriffs ein Laptop eines Mitarbeitenden war, der einer Phishing-Attacke zum Opfer gefallen ist oder dass eine Firewall nicht richtig konfiguriert wurde.

Abschliessend ist im Rahmen der «Detect und Respond»-Strategie die Bedeutung eines zeitnahen und zielgerichteten Reportings von Sicherheitsvorfällen hervorzuheben. Organisationen müssen dabei berücksichtigen, dass das neue Schweizer Informationssicherheitsgesetz (ISG)[7] eine Meldeplicht für Cyberangriffe auf kritische Infrastruktur vorsieht. Die Anwendbarkeit der Meldepflicht gilt es als Organisation zwingend zu ermitteln und dann auch einzuhalten. Die Meldung muss nicht nur zeitgerecht erfolgen, sondern auch Informationen zur Art und Ausführung des Cyberangriffs inkludieren. Diese können allerdings nur ermittelt werden, wenn eine Organisation auch die notwendige Nachvollziehbarkeit der Aktivitäten in System in ihrer Obhut besitzt, für die es eine funktionierende Überwachungs- und Analyseinfrastruktur benötigt.

In NIST CSF [3] korrespondiert die Überwachungsaktivität zu den Kategorien «Detect» und «Respond». Bei ISA/IEC-62443 taucht es zu organisatorischen Massnahmen vor allem unter «Incident Planning and Response» (ISA/IEC 62443-2-1, Kapitel 4.3.4.6) auf und unter technischen Massnahmen vor allem unter «Timely Reaktion to Events» (ISA/IEC 62443-3-1 Kapitel SR6). Für letzteres finden sich in Kapitel 5.6 der vorliegenden Empfehlung noch weitere Detailausführungen zu sinnvollen technischen Massnahmen.

Bei ISO 27001:2022 korrespondiert dies zur Kontrolle «8.16 Überwachungstätigkeiten» und ist damit Teil von Informationssicherheitsmanagementsystemen (ISMS) auf den Stand des aktuellen ISO27k Standards.

4.9.2. Best Practice Ansatz

Das Protokollieren (Logging) von Netzwerk-, System- und Anwendungsaktivitäten ist ein leistungsstarkes Mittel zur Abwehr von Cyberangriffen und sicherheitsrelevanten Vorfällen. Der Best Practice Ansatz ist, Überwachung und Reaktion («Detect and Respond») als integrierten Prozess zu betrachten, der sowohl den technologischen als auch organisatorischen Gegebenheiten der Organisation entspricht und eine rasche Reaktion auf Vorfälle ermöglicht. Zwar bieten zahlreiche Anbieter kostenpflichtige Tools und Dienste an, doch können auch weniger kostenintensive, aber dennoch effektive Ansätze mit Open-Source-Tools, integrierten Diensten wie «Syslog» und manueller Überwachung durch qualifiziertes Fachpersonal erfolgreich umgesetzt werden.

Die Einführung von Überwachung und Reaktion in der OT einer Organisation wird massgeblich dadurch unterstützt, wenn bereits ein ISMS auf Basis des Standards ISO-27001:2022 implementiert ist, welches der IT eine explizite Kontrolle über «Überwachungstätigkeiten» ermöglicht. In dem Fall können die bestehenden Sicherheitsmassnahmen zur Überwachung und Analysen auf die OT erweitert und bei Bedarf zusätzliche OT-spezifische Überwachungsgeräte integriert werden. Erfolgreiche Überwachungstätigkeiten erfordern zudem die gezielte Schulung der Mitarbeitenden zur effektiven Nutzung der verschiedenen Systeme. sowie die sorgfältige Erarbeitung und regelmässige Aktualisierung von «Runbooks» oder «Vorfallplänen».

«Detection and Response» ist eine häufig angebotene Cybersecurity-Dienstleistung, bei der sogenannte Security Operations Center (SOC) über ein zentrales Security Information and Event Management (SIEM) sowie verschiedenen Sensoren (z. B. IDS, EDR) Vorfälle erkennen und anschliessend mithilfe vorgefertigter «Runbooks» (Vorfallplänen) darauf reagieren.

Bei der Auswahl entsprechender Angebote sollte daher besonders auf das Kosten-Nutzen-Verhältnis geachtet werden, um sich nicht von der metaphorischen Welle von Angeboten überrollen zu lassen. Insbesondere bei SOC sind im OT-Umfeld der Nutzen und die Fähigkeit der Anbieter kritisch zu analysieren und den eigenen Bedürfnissen entgegenzustellen. Im heterogeneren OT-Umfeld wie der Gebäudeautomation fehlt es vielen SOC an notwendigem Fachwissen, da hier häufig hochspezialisierte Lösungen zum Einsatz kommen. Dies bedeutet auch, dass sich Lösungsansätze bei Vorfällen oder Problemen nicht einfach wiederverwenden lassen.

4.9.3. Praxisbeispiel

Um die Nützlichkeit einer Überwachungs- und Analyseinfrastruktur zu verdeutlichen – selbst, wenn sie kostengünstig und schlank gehalten ist - folgt ein Praxisbeispiel zur im Jahr 2021 bekannt gewordenen Sicherheitslücke in der Applikation «Log4j».

Für diese Sicherheitslücke wurden Standardangriffe entwickelt, die im sog. «Dark Web» weitverbreitet wurden. Diese wurden dann durch weniger fortgeschrittene Hacker

genutzt, um grossflächig diese Standardangriffe bei so vielen öffentlich zugänglichen Geräten zu probieren, in der Hoffnung, Endnutzer zu erwischen, die noch nicht die notwendigen Security Patches eingespielt haben.

Als möglicher Schutz dagegen kann z. B. «Fail2ban» genutzt werden, welches als Standardsoftware-Komponente bei Linux-basierten Betriebssystem einfach bezogen werden kann. Dies analysiert Logdateien eines Endgeräts mit leicht konfigurierbaren Filtern und konnte dadurch verlässlich die Signatur von Standardangriffe auf «Log4j» erkennen und blockieren. In dem Fall nutzt es die bereits existierenden Firewall-Systeme, z. B. «iptables» auf Linux-Maschinen, um den Angreifer mindestens temporär zu blockieren. Allein damit kann das Programm «Fail2ban» mit wenig Aufwand und kostenfrei eine grosse Anzahl von Angriffsversuchen anhand seiner Überwachung- und Analyseaktivitäten erkennen und verhindern.

4.10. Schwachstellen- und Patch Management

4.10.1. Sinn und Zweck

Im Zeitalter zunehmender Cyber-Bedrohungen gewinnt die OT-Sicherheit immer mehr an Bedeutung, da ein erfolgreicher Angriff auf Systeme schwerwiegende physische, finanzielle und sicherheitsrelevante Folgen haben kann. Best Practices aus der Branche bieten einen strukturierten Ansatz zur Stärkung der Sicherheitspraktiken in OT-Umgebungen und machen sie widerstandsfähiger gegen Cyberangriffe.

Ein zentraler Bestandteil eines effektiven Sicherheitsmanagementsystems für OT, basierend auf dem NIST CSF [3], ist das Software-Management, einschliesslich regelmässiger Updates (Patching). Diese Massnahme ist entscheidend, um Schwachstellen in OT-Systemen zu schliessen, die Betriebssicherheit zu gewährleisten und potenzielle Bedrohungen zu minimieren. Patching ist eine besondere Herausforderung in OT-Umgebungen aufgrund der bereits erwähnten verlängerten Lebenszyklen von Systemen, der Bereitstellung von Patches, der hohen Verfügbarkeitsanforderungen und der begrenzten geplanten Ausfallzeiten. Daher müssen Updates sorgfältig geplant und getestet werden, um sicherzustellen, dass sie die Betriebskontinuität nicht beeinträchtigen. Während das Softwaremanagement in IT-Umgebungen stark auf die Verfügbarkeit, Integrität und Vertraulichkeit von Daten ausgerichtet ist, hat das Softwaremanagement in OT-Umgebungen spezifische Anforderungen und Herausforderungen, die aus den einzigartigen Betriebsbedingungen und den physischen Konsequenzen eines Fehlers resultieren, wie beispielsweise

- **Sicherheitsprioritäten und Bedrohungslandschaft**: In IT-Umgebungen liegt der Fokus des Softwaremanagements häufig auf dem Schutz von Daten und der Sicherstellung der Verfügbarkeit von Diensten. In OT-Umgebungen hingegen stehen die physische Sicherheit und die Betriebssicherheit an erster Stelle. Angriffe auf OT-Systeme können nicht nur zu Datenverlusten, sondern auch zu physischen Schäden, Produktionsausfällen oder sogar zur Gefährdung von Menschenleben führen. Dementsprechend müssen die Sicherheitsmassnahmen in OT-Umgebungen sowohl auf die Prävention von Cyber-Angriffen als auch auf die Vermeidung physischer Störungen ausgerichtet sein. Bereits bei der Beschaffung von OT-Systemen sollte darauf geachtet werden, dass klare Vereinbarungen mit dem Lieferanten und Integrator über die Bereitstellung und Implementierung von Sicherheitsupdates bestehen. Sicherheitsupdates, wie Major- und Minor-Patches, sollten als Voraussetzung für Wartungsverträge festgelegt werden, um sicherzustellen, dass die Systeme regelmässig aktualisiert und geschützt bleiben. Ein gutes Patchmanagement erfordert zudem die klare Definition von Verantwortlichkeiten. So sollte der Lieferant mindestens zweimal jährlich über Major-Patches informieren, während der Integrator den Betreiber über sowohl Major- als auch Minor-Patches in Kenntnis setzt. Innerhalb des Unternehmens ist eine verantwortliche Rolle zu definieren, die kontinuierlich Sicherheitslücken überprüft und sicherstellt, dass die erforderlichen Updates zeitnah eingespielt werden.
- **Update- und Patch-Management**: Während IT-Systeme normalerweise regelmässig und automatisch mit Sicherheitsupdates versorgt werden können, erfordert das Patch-Management in OT-Umgebungen eine viel sorgfältigere Planung. Dies liegt daran, dass viele OT-Systeme kontinuierlich in Betrieb sind und nicht ohne weiteres angehalten oder neu gestartet werden können, um Updates durchzuführen. Ein unbedachtes Update könnte die Funktionsfähigkeit kritischer Systeme beeinträchtigen und erhebliche Störungen verursachen.
- **Lebenszyklus-Management und Legacy-Systeme**: IT-Systeme haben oft kürzere Lebenszyklen und werden regelmässig aktualisiert oder ersetzt, um mit technologischen Fortschritten Schritt zu halten. OT-Systeme hingegen sind häufig auf Langlebigkeit ausgelegt und können jahrzehntelang im Einsatz bleiben. Dies führt dazu, dass viele OT-Systeme auf älteren, möglicherweise anfälligeren Softwareversionen basieren, was zusätzliche Herausforderungen für das Sicherheitsmanagement mit sich bringt. Sicherheitsmassnahmen müssen daher häufig auf ältere Technologien abgestimmt und gegebenenfalls spezielle Schutzmassnahmen entwickelt werden, z. B. Härtungsmassnahmen, wie Whitelisting von Applikationen, strengere Zugriffskontrolle zum System, restriktivere Firewall Einstellungen, usw.

4.10.2. Best Practice Ansatz

Best Practices im Patch-Management sind entscheidend, um die Sicherheit und Stabilität von IT- und OT-Systemen zu gewährleisten. Die folgenden Tipps können bei einer erfolgreichen Patchmanagement-Strategie helfen.

- Die Identifizierung von Schwachstellen umfasst die kontinuierliche Überwachung neuer Schwachstellen aus verschiedenen Quellen wie Herstellerankündigungen, Sicherheitshinweisen und Schwachstellendatenbanken. Dabei werden potenzielle Schwachstellen erfasst und bewertet, um die möglichen Auswirkungen auf die Unternehmenswerte zu bestimmen und geeignete Massnahmen zur Risikominimierung zu ergreifen.

- Bevor Patches auf den Produktionssystemen installiert werden, sollten sie in einer kontrollierten Umgebung, wie einer Integrations- oder Testumgebung, gründlich getestet werden. Dies stellt sicher, dass die Patches keine negativen Auswirkungen auf die Systemfunktionalität haben. Die Ergebnisse dieser Tests, einschliesslich aller aufgetretenen Probleme und deren Lösungen, sollten sorgfältig dokumentiert werden.
- Die Bereitstellung von Patches muss einem formellen Change Management Prozess folgen, um die notwendige Genehmigung zu erhalten. Es muss sichergestellt werden, dass nur autorisiertes Personal die Berechtigung hat, Systemänderungen vorzunehmen, einschliesslich der Installation von Patches, um die Integrität der Systeme zu wahren.
- Die Planung und Terminierung der Patch-Bereitstellung sollten so erfolgen, dass die Beeinträchtigung des Geschäftsbetriebs minimiert wird. Die Patches müssen gemäss dem genehmigten Zeitplan auf den Produktionssystemen implementiert werden, um eine effiziente und sichere Aktualisierung zu gewährleisten.
- Nach der Installation von Patches muss überprüft und protokolliert werden, ob diese auf allen Zielsystemen erfolgreich installiert wurden. Zudem sollten Post-Deployment-Tests durchgeführt werden, um sicherzustellen, dass die Systeme nach der Patch-Anwendung ordnungsgemäss funktionieren und keine neuen Probleme aufgetreten sind. Nachher sollten Systeme kontinuierlich auf Probleme oder Anomalien überwacht werden. Regelmässige Berichte über den Status der Patch-Management-Aktivitäten sollten an die zuständigen Stellen weitergeleitet werden, um Transparenz und Kontrolle zu gewährleisten.
- Der Patch-Management-Prozess sollte regelmässig überprüft werden, um Bereiche zu identifizieren, die verbessert werden könnten. Es ist wichtig, das Feedback der Beteiligten sowie die gesammelten Erfahrungen zu nutzen, um die Patch-Management-Strategie kontinuierlich zu verbessern. Darüber hinaus sollte ein Lifecycle Management betrieben werden, um den Umgang mit angekündigten Plattformen zu planen und festzulegen.

4.10.3. Praxisbeispiel

Ein aktuelles Beispiel für einen Sicherheitsvorfall im Bereich OT-Sicherheit und Patch-Management ist der Colonial Pipeline Cyberangriff von 2021. Obwohl sich der Angriff primär auf IT-Systeme richtete, verdeutlicht er die enge Verbindung zwischen IT- und OT-Infrastrukturen und zeigt, wie schwerwiegende Folgen eine Vernachlässigung von Sicherheitsmassnahmen, einschliesslich des Patch-Managements, haben kann.

Im Mai 2021 wurde Colonial Pipeline, eines der grössten Pipeline-Netzwerke in den USA und das 45% des Treibstoffs an die Ostküste liefert, Opfer eines Ransomware-Angriffs der Hackergruppe DarkSide. Der Angriff traf vorrangig die IT-Systeme, aber die Konsequenzen zwangen das Unternehmen dazu, den Betrieb der Pipeline zu stoppen, um die OT-Systeme vor einer möglichen Infektion zu schützen. Die Angreifer nutzten Schwachstellen in den IT-Systemen aus, die durch regelmässiges Patchen hätten geschlossen werden können. Ein ungepatchter VPN-Zugang, der für Remote-Mitarbeitende eingerichtet war, ermöglichte den Hackern den Zugriff auf das Netzwerk. Die Ransomware führte zur Verschlüsselung von IT-Daten, woraufhin der Betrieb der Pipeline vorsichtshalber eingestellt wurde, um die OT-Infrastruktur zu schützen.

Der Stillstand der Pipeline führte zu erheblichen Unterbrechungen in der Treibstoffversorgung an der US-Ostküste, was Panikkäufe, Engpässe und einen starken Anstieg der Kraftstoffpreise zur Folge hatte. Um den Zugriff auf die Daten wiederherzustellen, zahlte

das Unternehmen eine Lösegeldsumme von etwa 4.4 Millionen US-Dollar, doch die direkten und indirekten Kosten des Vorfalls waren weitaus höher.

Der Angriff verdeutlicht die Bedeutung von Patch-Management und die Gefahren ungepatchter Systeme. Der Einbruch erfolgte über einen nicht gesicherten VPN-Zugang, was zeigt, dass veraltete Software und fehlende Updates bei kritischen Infrastrukturen schwerwiegende Auswirkungen auf OT-Systeme haben können, auch wenn der Angriff primär auf IT-Systeme abzielt. Die enge Verbindung zwischen IT und OT wird hier ebenfalls deutlich, da ein Angriff auf IT-Systeme den OT-Betrieb vollständig lahmlegen kann. Regelmässige Sicherheitsupdates, strenge Schutzmassnahmen und die Sicherung von Remote-Zugängen, etwa durch Multi-Faktor-Authentifizierung, hätten möglicherweise den Angriff verhindern können.

4.11. Audit und Bewertung

4.11.1. Sinn und Zweck

Der Prozess des Audits und der Bewertung von OT-Infrastrukturen im Bereich der Sicherheit verfolgt das Ziel, potenzielle Schwachstellen und Risiken in industriellen Systemen frühzeitig zu erkennen und gezielt zu reduzieren. Dies ist vor allem für die Aufrechterhaltung eines hohen Sicherheitsniveaus in kritischen Infrastrukturen unerlässlich, da hier oft sicherheitsrelevante Prozesse gesteuert und überwacht werden.

Durch Audits und Bewertungen, die auf diesen Standards basieren, können Organisationen ihre OT-Infrastruktur systematisch überprüfen, bestehende Sicherheitslücken identifizieren und gezielte Massnahmen ergreifen. So tragen sie entscheidend dazu bei, das Risiko von Cyber-Angriffen auf industrielle Systeme zu verringern und die Sicherheit ihrer kritischen Prozesse zu gewährleisten.

Das NIST CSF [3] 2.0 und der ISA/IEC 62443-Standard bieten hierfür eine umfassende Grundlage. Das NIST CSF definiert fünf Kernfunktionen («Identify», «Protect», «Detect», «Respond» und «Recover»), die es Unternehmen ermöglichen, systematische Sicherheitsmassnahmen aufzubauen und kontinuierliche Verbesserungen umzusetzen. Ergänzend dazu bietet IEC 62443 spezifische Anforderungen für die OT-Sicherheit in industriellen Automatisierungs- und Steuerungssystemen (IACS). Dieser Standard richtet sich an Hersteller, Betreiber und Integratoren und beschreibt eine klare Vorgehensweise, um Bedrohungen gezielt zu begegnen und Risiken im industriellen Umfeld zu minimieren.

4.11.2. Best Practice Ansatz

Die folgende Checkliste unterstützt die effektive Umsetzung einer OT-Sicherheitsstrategie, damit durch ein strukturiertes und standardisiertes Vorgehen sichergestellt wird, dass alle relevanten Aspekte systematisch überprüft werden. Diese hilft, Schwachstellen frühzeitig zu identifizieren, Ressourcen effizient zu nutzen und die Konsistenz bei Sicherheitsmassnahmen zu wahren. Die Dokumentation der durchgeführten Massnahmen fördert Nachvollziehbarkeit und unterstützt bei der Einhaltung von Vorschriften. Zudem ermöglicht die Checkliste kontinuierliche Verbesserungen und erleichtert die Kommunikation und Zusammenarbeit innerhalb des Teams. In Krisensituationen bietet sie klare Handlungsanweisungen und trägt zur effizienten Reaktion bei.

Empfehlung	Beschreibung
Inventarisierung und Dokumentation	Sind alle OT-Assets (Hardware, Software, Firmware, Netzwerkinfrastruktur, IoT-Geräte) vollständig inventarisiert? Werden die Inventarlisten regelmässig aktualisiert? Gibt es eine umfassende Dokumentation zu Herstellerinformationen, Modellnummern, Seriennummern, Installationsorten, Konfigurationen und Softwareversionen? Ist eine Kritikalitätsbewertung der OT-Assets durchgeführt worden?
Überwachung und Bewertung	Sind Monitoring-Tools implementiert, um den Zustand und die Leistung der OT-Assets in Echtzeit zu überwachen? Werden regelmässige physische und digitale Audits durchgeführt, um Sicherheitsstandards zu überprüfen? Gibt es einen Prozess zur regelmässigen Schwachstellenbewertung und Behebung von Sicherheitslücken?
Patch-Management und Software-Updates	Existiert ein dokumentierter Patch-Management-Prozess? Werden Patches und Updates regelmässig überprüft und angewendet? Gibt es eine Testumgebung, um Patches vor der Implementierung zu testen?
Change Management	Ist ein strukturierter Änderungsmanagementprozess vorhanden? Werden alle Änderungen an OT-Assets sorgfältig geprüft, genehmigt und dokumentiert? Gibt es Risikobewertungen für geplante Änderungen? Sind Rollback-Pläne vorhanden, um Änderungen rückgängig zu machen, falls notwendig?
End-of-Life-Management	Werden der Lebenszyklusstatus und das End-of-Life von OT-Assets regelmässig überwacht? Gibt es Strategien für den Austausch veralteter oder nicht mehr unterstützter Geräte und Software? Werden Daten sicher entfernt und gelöscht, um die Sicherheit zu gewährleisten?
Schulung und Sensibilisierung	Werden regelmässige Schulungen für alle Mitarbeiter, die mit OT-Systemen arbeiten, durchgeführt? Sind Awareness-Programme zur OT-Sicherheit implementiert? Werden die Mitarbeiter regelmässig zu neuen Bedrohungen und Sicherheitsverfahren informiert?
Kontinuierliche Verbesserung	Werden die OT-Sicherheitsprozesse regelmässig überprüft und aktualisiert? Ist ein Feedback-Mechanismus implementiert, um aus Vorfällen zu lernen und die Strategie zu verbessern? Gibt es eine umfassende Dokumentation aller Prozesse, Änderungen und Vorfälle?
Notfallpläne und Wiederherstellung	Existieren Notfallpläne für OT-Systeme (Desaster Recovery Plan und Business Continuity Plan)? Werden die Wiederherstellungsprozesse regelmässig getestet und aktualisiert? Gibt es klare Kommunikationswege und Verantwortlichkeiten für den Fall eines Sicherheitsvorfalls?
Technologische Schutzmassnahmen	Gibt es eine ausreichend sichere Segmentierung des Netzes? Sind Firewalls und Netzwerksicherheitsmassnahmen implementiert und aktuell? Wird ein regelmässiges Vulnerability Management durchgeführt? Werden die Systeme auf Bedrohungen und ungewöhnliche Aktivitäten überwacht?

Compliance und Reporting	Werden alle rechtlichen und regulatorischen Anforderungen im Bereich OT-Sicherheit erfüllt? Sind Verfahren zur internen und externen Berichterstattung von Vorfällen etabliert? Werden alle sicherheitsrelevanten Aktivitäten und Vorfälle protokolliert und dokumentiert?

Tabelle 4: Checkliste für die effektive Umsetzung einer OT-Sicherheitsstrategie

4.11.3. Praxisbeispiel

Ein relevantes Praxisbeispiel hier ist der Norsk Hydro-Vorfall im Jahr 2019, bei dem der norwegische Aluminiumhersteller erfolgreich auf einen Cyberangriff reagierte und durch vorbereitende Sicherheitsmassnahmen grössere Schäden verhindern konnte. Norsk Hydro wurde von einem LockerGoga-Ransomware-Angriff getroffen, der sowohl IT- als auch OT-Systeme betraf. Der Angriff zwang das Unternehmen, einige seiner automatisierten Anlagen vorübergehend auf manuelle Steuerung umzustellen, um den Betrieb aufrechtzuerhalten.

Bereits vor dem Angriff hatte Norsk Hydro regelmässig Audits und Bewertungen seiner kritischen Infrastrukturen und Sicherheitsmassnahmen durchgeführt, die auf Standards wie dem NIST CSF basierten. Diese vorbereitenden Audits halfen dem Unternehmen, Schwachstellen frühzeitig zu erkennen und gezielte Schutzmassnahmen zu implementieren, darunter die Segmentierung der Netzwerke, die Einführung redundanter Systeme und die Erstellung eines detaillierten Notfallplans.

Diese Sicherheitsvorkehrungen erwiesen sich als entscheidend, da Norsk Hydro in der Lage war, den Betrieb auf alternativen Wegen aufrechtzuerhalten und den Schaden zu begrenzen. Der Angriff kostete das Unternehmen zwar einige Millionen Euro, doch durch die getroffenen Vorbereitungen und die schnellen Reaktionsmassnahmen konnte ein kompletter Stillstand und ein grösserer wirtschaftlicher Schaden vermieden werden.

Das Beispiel Norsk Hydro zeigt die Bedeutung von regelmässigen Audits und Bewertungen, um Unternehmen widerstandsfähiger gegen Cyberangriffe zu machen. Es führte zu einer breiten Anerkennung der Wichtigkeit von OT-Sicherheit in der Industrie und ermutigte andere Unternehmen, ihre Auditing-Prozesse zu intensivieren und ihre Sicherheitsstrategien zu überarbeiten.

5. Technische Vorgaben

5.1. Risikobasierte IKT-Sicherheitsmassnahmen, abgeleitet von Anforderungen

Nicht jede Norm muss in ihrer Gesamtheit übernommen werden – entscheidend ist, dass gezielt jene Aspekte ausgewählt und angewendet werden, die im jeweiligen Umfeld einen konkreten Mehrwert bieten. Im Kontext der IKT-Sicherheit bedeutet das, dass Schutzmassnahmen nicht pauschal, sondern risikobasiert abgeleitet und umgesetzt werden sollen.

Die vorliegende Empfehlung orientiert sich für die technischen Massnahmen wieder an dem gängigen OT-Security Standard ISA/IEC-62443, spezifisch ISA/IEC-62443-3-3 [5]. Dieser empfiehlt technische Massnahmen für Schutzobjekte und Gruppen von Schutzobjekte anhand des jeweiligen Sicherheitsbedarf von sieben spezifischen Anforderungen an die IKT-Sicherheit abzuleiten. Diese Anforderungen sind eine Erweiterung der klassischen Informationssicherheitstriade CIA (**C**onfidentiality, **I**ntegrity, **A**vailability, auf Deutsch Vertraulichkeit, Integrität, Verfügbarkeit). Nebst der CIA inkludiert es jeweils die Zugriffs- und Nutzungskontrolle, die Limitierung von Datenflüssen sowie die zeitnahe Reaktion auf Vorfälle.

Dieser Ansatz erlaubt die risikobasierte Definition von Massnahmen und die Fokussierung von Aufwand und Komplexität der Massnahmen auf die entscheidenden Anforderungen und Schutzbedarfe. Für detaillierte Identifikation von Massnahmen kann auf ISA/IEC-62443-3-3 [5] zugegriffen werden. In dieser Empfehlung wird allerdings der Fokus auf eine kleinere Anzahl von technischen Massnahmen gesetzt, welche generisch sinnvoll für Projekte mit Gebäudeautomation sind. Anschliessend sollten im Rahmen der organisatorischen Massnahmen und des risikobasierten Sicherheitsmanagementsystems – abhängig vom jeweiligen Projektkontext – zusätzliche technische Massnahmen für bereits identifizierte aber bislang unbehandelte Risiken definiert werden, für die derzeit noch keine Gegenmassnahmen existieren.

Da das in dieser Empfehlung beschriebene Sicherheitsmanagementsystem kein ISA/IEC-62443-3 «Cyber Security Management System» sein muss, empfiehlt dieses Dokument ein risikobasiertes Tailoring für Bauherren. Wie in Kapitel 4.1 beschrieben, beginnt die Massnahmendefinition mit einer Risikobewertung. Hierfür empfiehlt es sich eine Übersicht über sogenannte «System under Scope» zu schaffen, um dann ein simplifiziertes Zonenkonzept zu definieren. Hierfür werden die involvierten IKT-Schutzobjekte des «System under Scope» in die Schutzbedarfskategorien «Normal» und «Erhöht» aufgeteilt. Für diese Schutzbedarfsanalyse kann die gängige HERMES-Version genutzt werden. Alternativ wird je Zone, d.h. eine Gruppierung von ähnlich kritischen IKT-Schutzobjekten, als «Normal» betrachtet und mit den regelmässigen Sicherheitsmassnahmen behandelt, ausser es wird für die Zone identifiziert, dass sie in mindestens einer der sieben Sicherheitsanforderungen nach ISA/IEC-62443-3-3 einen erhöhten Schutzbedarf hat. In diesem Fall würde die Zone als «Erhöht» definiert und die konkreten Sicherheitsanforderungen ausgewiesen, wo erhöhter Sicherheitsbedarf besteht.

Zur Demonstration dieses Ansatzes folgt ein Praxisbeispiel: Die Beleuchtung eines Raumes, welche durch die Gebäudeautomation gesteuert wird. Die betroffenen IKT-Schutzobjekte lassen sich in zwei Kategorien unterteilen: die reguläre Beleuchtung für die normalen Nutzung des Raumes, sowie die Notbeleuchtung. In Tabelle 5 wird der Schutzbedarf dieser beiden Gruppen oder «Zonen» entlang der sieben Sicherheitsanforderungen analysiert und ausgewiesen.

Sicherheitsanforderung	Zone 1: Bürolüftung	Zone 2: RWA-Fluchtweg
Identifikations- und Authentifikationskontrolle	Normal: Zugriff durch interne Mitarbeitende oder Gebäudetechnik ist ausreichend.	Erhöht: Zugriff nur durch definiertes Fachpersonal.
Nutzungskontrolle	Normal: Änderungen an den Lüftungseinstellungen sind durch Benutzer oder Facility-Management erlaubt.	Erhöht: Zugriff nur durch definiertes Fachpersonal, damit die Verfügbarkeit nicht durch Falschnutzung oder Arglist gefährdet wird.
Systemintegrität	Normal: Fehlsteuerungen und Ausfälle beeinträchtigen den Komfort, sind aber betrieblich unkritisch.	Erhöht: Die RWA muss im Ernstfall zuverlässig funktionieren. Manipulationen oder Ausfälle können lebensgefährlich sein.
Datenvertraulichkeit	Normal: Betriebsdaten der Lüftung sind in der Regel unkritisch.	Normal: Betriebsdaten der RWA sind in der Regel unkritisch.
Eingeschränkter Datenfluss	Normal: Mehr als eine Aufteilung in Subnetze zum Auseinanderhalten von Feldgeräten ist hier nicht notwendig.	Erhöht: Da diese Zone Schutzgeräte inkludiert, muss die von den normalen Datenflüssen separat gehalten werden, u.a. um einen Dominoeffekt von unkritischen Vorfällen in Zone 1 zu einem kritischen Vorfall in Zone 2 zu verhindern.
Zeitnahe Reaktion auf Vorfälle	Normal: Ausfälle werden durch das System oder Mitarbeitenden bemerkt und eine Instandsetzung wird je nach Kontext priorisiert eingeplant und zeitnah nachgegangen.	Erhöht: Ein Ausfall ist immer kritisch. Fehler oder Ausfälle müssen sofort erkannt, gemeldet und behoben werden (z. B. durch 24/7-Überwachung und Alarmierung).
Verfügbarkeit von Ressourcen	Normal: Ausfälle beeinträchtigen den Komfort, sind aber betrieblich unkritisch.	Erhöht: Ausfall der RWA kann im Brandfall Menschenleben gefährden – höchste Verfügbarkeitsanforderung.
Identifizierter Schutzbedarf	Normal	Erhöht
Resultierende Massnahmen	Standardmässige Netzwerksicherheit und Zugriffskontrolle.	Erweiterte Sicherheitsmechanismen: Segmentierung, Authentifizierung, Überwachung, Notfallpläne, dokumentierte Wartung.

Tabelle 5: Beispiel für die vorgeschlagene Schutzbedarfsanalyse

Die Schutzbedarfsanalyse ergibt in diesem Fall, dass die Zone 1, die reguläre Raumbeleuchtung, einen «normalen Schutzbedarf» aufweist. Im Gegensatz dazu hat Zone 2, die Notbeleuchtung, einen «erhöhten Schutzbedarf», was zusätzliche Massnahmen erforderlich macht. Hier fokussiert man sich aber auf Massnahmen, welche Sicherheitsanforderungen ansprechen, die einen «erhöhten Schutzbedarf» haben.

So könnte man für Zone 2 den «erhöhten Schutzbedarf» wie folgt handhaben: Die Notbeleuchtung ist an die Notstromzufuhr angeschlossen, ihre Abschaltung ist nur physisch möglich, indem sie von der Stromzufuhr durch autorisiertes Personal getrennt wird. Sollte sie ausfallen, löst dies einen Alarm bei der Gebäudeverwaltung aus. Diese pragmatische Lösung wird den Anforderungen der IKT-Sicherheit gerecht und bedarf trotzdem keine hochkomplizierte Lösung.

Ein weiteres Beispiel ist die Kühlung der Büroräumlichkeiten mit normalen Schutzbedarf und die Kälteversorgung für Datacenter mit erhöhtem Schutzbedarf.

5.2. Identifikations-, Authentifikations-, und Nutzungskontrolle (AC/UC)

Bei der Identifikations- und Authentifikationskontrolle wird die Identität eines Nutzers überprüft und die Zugriffsrechte des identifizierten Nutzers verifiziert. Ein Nutzer kann ein Mensch, ein Softwareprozess oder ein Gerät umfassen. Die Nutzungskontrolle bündelt dann die Autorisierungskontrolle, sowie das Sicherstellen der Nachvollziehbarkeit der verschiedenen Aktivitäten.

Gemeinsam bündelt diese drei Kontrollen das Thema «Identity & Access Management» (IAM), wobei dies im OT-Umfeld der Gebäudeautomation oft nur limitiert durch die involvierte Technik unterstützt wird. So hat z. B. BACnet/IP keine Fähigkeit, Nutzer zu identifizieren und zu authentifizieren. Damit kann es auch nicht nutzerspezifische Berechtigungen definieren bzw. die Kommunikation nutzerspezifisch einschränken. Dies ist bei den allermeisten Gebäudeautomation-Systemen und -protokollen auch der Fall, weswegen die Thematik «IAM» vorwiegend auf der Leitebene der Gebäudeautomation realisiert werden muss.

Innerhalb von OT-Netzen ist eine derartige Zugriffs- und Nutzungskontrolle oft nicht möglich. Deswegen ist diese am und bis zum sogenannten Perimeter zwischen den Gebäudeautomation-Netze sicherzustellen, z. B. durch geschützte Zugriffsmechanismen via VPNs oder durch die lokale Verifikation von Geräten via einem sogenannten Network Access Control (NAC). Gleichzeitig muss dann, wie in Kapitel 5.5 beschrieben, die Netzwerksegmentierung und -isolierung, als kompensierte Massnahme genutzt werden.

Als weitere kompensierte Massnahme fungiert die Sicherstellung eines nachvollziehbaren und abgestimmten Change Management, welches die gewollten Änderungen an Geräten kontrolliert und dokumentiert. Technisch wird dies unterstützt von Audit Logging Systeme, welche die verschiedenen Veränderungen datiert dokumentiert auf sog. «unveränderlichen Speicher». Damit wird unter anderem auch verhindert, dass bei einem Cyberangriff dessen Evidenzen gelöscht werden können. Dies erlaubt dann auch eine nachträgliche Zugriffs- und Nutzungskontrolle.

5.3. Systemintegrität (SI)

5.3.1. Sinn und Zweck

Systemintegrität bezieht sich auf die Fähigkeit eines Systems, seine korrekte Funktionsweise sicherzustellen und unbefugte Änderungen zu verhindern, indem es vor Manipulationen geschützt ist und seine Daten und Prozesse unverändert bleiben. Dies umfasst Anforderungen wie:

- **Kommunikationsintegrität**: Es gilt die Integrität der Kommunikation sicherzustellen, indem unbefugte Änderungen, Abhörversuche und Manipulationen während der Datenübertragung verhindert werden.
- **Schutz vor Schadcode:** Es sind Mechanismen zu implementieren, die das Eindringen und die Ausführung von Schadsoftware verhindern, um die Integrität des Systems zu gewährleisten.
- **Verifikation der IT-Sicherheitsfunktionalität:** Es ist regelmässig zu überprüfen und zu bestätigen, dass alle IT-Sicherheitsfunktionen korrekt und wie beabsichtigt arbeiten, um die Integrität des Systems zu gewährleisten.
- **Software- und Informationsintegrität:** Es ist die Integrität von Software und Informationen sicherzustellen, indem unbefugte Änderungen und Manipulationen verhindert werden.
- **Eingabevalidierung:** Alle Eingaben sind zu überprüfen und zu validieren, um sicherzustellen, dass sie korrekt und autorisiert sind, bevor sie verarbeitet werden.
- **Vorbestimmte Zustände der Ausgänge:** Im Falle eines Fehlers oder einer Störung muss in einen sicheren, vorher festgelegten Zustand gewechselt werden, um die Integrität und Sicherheit des Systems zu gewährleisten.
- **Fehlerbehandlung:** Fehler sollen erkannt, gemeldet und behoben werden, um die Integrität des Systems aufrechtzuerhalten.
- **Sitzungsintegrität:** Die Kommunikation auf Sitzungsebene muss geschützt werden, um Vertrauen in die Identität und Gültigkeit der Informationen an beiden Enden der Sitzung zu gewährleisten.

Ein Beispiel, wie die Systemintegrität kompromittiert werden kann, ist ein Man-in-the-Middle (MitM) Angriff. Bei einem MitM-Angriff schaltet sich ein Angreifer zwischen zwei kommunizierende Geräte, ohne dass diese es bemerken. Der Angreifer kann dann den Datenverkehr abfangen, manipulieren oder sogar eigene Daten einfügen.

Szenario: Ein Angreifer platziert ein Gerät in einem ungesicherten Netzwerksegment und fängt die Kommunikation zwischen einem AS-Controller und einem Sensor ab. Der Angreifer kann dann die Sensordaten manipulieren, was zu falschen Entscheidungen des Controllers führt, wie z. B. das Abschalten von Sicherheitssystemen oder das Auslösen von Alarmen.

Ein weiteres Beispiel, Malware-Infektion: Hacker können Malware einschleusen, welche die Integrität von Software und Daten verändern. Dies kann durch Phishing-Angriffe oder das Ausnutzen von Sicherheitslücken geschehen.

5.3.2. Best Practice Ansatz

Um die Systemintegrität zu gewährleisten, gibt es mehrere bewährte Methoden und Technologien:

Empfehlung	Beschreibung
Verwendung von VPNs (Virtual Private Networks)	Verwendung von VPNs (Virtual Private Networks), um eine sichere und verschlüsselte Verbindung zwischen den Geräten zu gewährleisten. Dadurch werden die Daten während der Übertragung vor Abhören und Manipulation geschützt. Besonders in unsicheren Netzwerken ist dies die sicherste Methode zur Übertragung von BACnet/IP-Daten, wenn BACnet/SC nicht verfügbar ist.
MAC-Filterung	Durch die Implementierung von MAC-Filterung wird der Netzwerkzugriff auf Geräte mit spezifischen MAC-Adressen beschränkt. Dies trägt zur Erhöhung der Sicherheit bei, indem unautorisierte Geräte ausgeschlossen werden. Allerdings können Angreifer MAC-Adressen durch MAC-Spoofing fälschen. Daher sollte MAC-Filterung nur als eine von mehreren Sicherheitsmassnahmen betrachtet werden, die implementiert werden sollten. (MAC – Media Access Control).
Physischer Zugangsschutz an allen Knoten	Physischer Zugangsschutz an allen Knoten (wie z. Bsp. Switches) und Endpunkten (z. Bsp. Sensoren, Steuerungspanel oder Computer), sodass nur autorisiertes Personal Zugang erhält. Dies kann durch Zugangskontrollen, Überwachungskameras und physische Barrieren erreicht werden.
Unbenutzte Ports	Unbenutzte Ports (wie RJ45-, serielle- oder USB-Anschlüsse) an Knoten und Endpunkten, sollen entweder deaktiviert oder physisch blockiert werden.
Kontinuierliche Überwachung	Eine kontinuierliche Überwachung und Protokollierung der Systemaktivitäten helfen, verdächtige Aktivitäten frühzeitig zu erkennen und darauf zu reagieren. Dies kann beispielsweise mit Firewalls und Intrusion Detection Systems (IDS) erreicht werden.
Netzwerksegmentierung	Wenn das Netzwerk in kleinere, isolierte Abschnitte oder Subnetze unterteilt wird, trägt dies dazu bei, die Integrität und Sicherheit des Netzwerks zu erhöhen. Siehe Kap. 5.5 Eingeschränkter Datenfluss.
Abnahme und Wartung	Bei der Abnahme der installierten Anlage und während geplanter Wartungsarbeiten sind die erforderlichen Sicherheitsmassnahmen zu überprüfen.
End-Point-Protection	Blockierung von CodeExecution, auch bekannt als Allowlisting oder Whitelisting stellt sicher, dass nur autorisierte Anwendungen und Prozesse auf einem System ausgeführt werden dürfen. Dies blockiert beispielsweise die Ausführung von schädlicher Software wie Malware. Antiviren- und Antimalware-Software erkennen und blockieren schädliche Software, bevor sie Schaden anrichten kann.
Eingabevalidierung	Eingabevalidierung bezieht sich auf die Überprüfung und Bereinigung von Benutzereingaben, zum Beispiel auf einer BACnet Operator Workstation, um sicherzustellen, dass diese den erwarteten Formaten und Werten entsprechen, bevor sie weiterverarbeitet werden.
Intrusion Detection System (IDS)	Ein IDS überwacht kontinuierlich den Netzwerkverkehr und die Systemaktivitäten, um verdächtige Muster und Anomalien zu erkennen. Dies hilft, Angriffe frühzeitig zu identifizieren, bevor sie Schaden anrichten können. Wenn ein IDS eine potenzielle Bedrohung erkennt, sendet es sofortige Alarme an die Systemadministratoren. Dies ermöglicht eine schnelle Reaktion und die Implementierung von Gegenmassnahmen, um die Integrität des Systems zu schützen.

Vorbestimmte Zustände der Ausgänge	Das festgelegte Verhalten der Ausgänge eines Automatisierungssystems im Falle von Angriffen ist entscheidend, um die Integrität des normalen Betriebs zu gewährleisten. Idealerweise fährt das Automatisierungssystem trotz eines Angriffs mit dem normalen Betrieb fort. Wenn es diesen jedoch nicht länger aufrechterhalten kann, müssen seine Ausgänge auf einen vorbestimmten Zustand zurückfallen. Der geeignete vorbestimmte Zustand des Automatisierungssystems hängt von der Anwendung ab und könnte eine vom Nutzer zu konfigurierende Option sein.

Tabelle 6: Checkliste für die Gewährleistung der Systemintegrität

5.3.3. Praxisbeispiel

Ein Cyber-Vorfall, der die Systemintegrität in der OT betrifft, ist der Angriff auf die Wasseraufbereitungsanlage in Oldsmar, Florida, im Februar 2021. Ein Hacker soll versucht haben, das Wasser in der Wasseraufbereitungsanlage zu vergiften, wobei letzte Erkenntnisse einräumen, dass es einen solchen Angriff nie gab. Dennoch bleibt dies ein wichtiges Beispiel für potenzielle Angriffe auf kritische Infrastruktur, welche auf Schwachstellen in der OT-Sicherheit abzielen.

Art des Angriffs: Ein unbekannter Angreifer verschafft sich über eine Fernzugriffssoftware Zugang zum Steuerungssystem der Wasseraufbereitungsanlage. Dabei werden schlechte Passwörter genutzt und für den Fernzugriff wird TeamViewer auf einer Windows 7 Maschine verwendet.

Auswirkungen: Der Angreifer versucht, die Menge an Natriumhydroxid (Lauge) im Wasser drastisch zu erhöhen, was die Wasserqualität gefährdet.

Auflistung einiger Security-Massnahmen, welcher zur Verhinderung des Angriffs hilfreich sind:

- **Verwendung sicherer Betriebssysteme, Aktualisierung und Patches**
  Die Sicherheitsupdates (Patches) für Windows 7 wurden am 14.11.2020 eingestellt. Der Einsatz eines aktuellen Betriebssystems und die Durchführung von regelmässigen Patches trägt dazu bei, viele bekannte Sicherheitslücken zu schliessen. Aber auch die verwendete Software muss regelmässig aktualisiert und auf Sicherheitslücken geprüft werden, da veraltete oder unsichere Applikationen Einfallstore für Angriffe darstellen können.
- **Verwendung starker Passwörter**
  Schwache Passwörter sind ein wesentliches Sicherheitsrisiko. In diesem Fall hätte die Verwendung von komplexen, einzigartigen Passwörtern den Angriff zumindest erschwert.
- **Multi-Faktor-Authentifizierung**
  TeamViewer und andere Remote-Access-Tools sollten mit Multi-Faktor-Authentifizierung gesichert werden, um sicherzustellen, dass ein Angreifer nicht nur mit einem Passwort Zugang erhält.
- **Kontinuierliche Überwachung des Netzwerkverkehrs**
  Eine umfassende Überwachung der Netzwerke und Systeme hätte frühzeitig verdächtige Aktivitäten wie ungewöhnlichen Zugang zu kritischen Systemen oder plötzliche Änderungen an den Chemikalienmengen erkannt.

- **Automatisierte Alarme bei ungewöhnlichen Aktivitäten**
  Das System hätte so konfiguriert werden müssen, dass es automatisch Alarm schlägt, wenn kritische Parameter wie die Menge an Natriumhydroxid verändert werden.
- **Zugriff nur bei Bedarf (Least Privilege)**
  Der Remote-Zugang hätte auf die notwendigen Funktionen und das Minimum an Berechtigungen beschränkt werden sollen. Nur autorisierte Mitarbeitende mit klar definierten Rollen sollten Zugriff auf die relevanten Systeme haben, und auch nur dann, wenn es unbedingt erforderlich ist.
- **Schulung zu Cybersicherheit**
  Regelmässige Schulungen für alle Mitarbeitende in der Wasseraufbereitungsanlage hinsichtlich sicherer Praktiken für die Nutzung von Remote-Tools und der sicheren Verwaltung von Passwörtern ist sehr wichtig.
- **Eingabevalidierung**
  Eine Eingabevalidierung hätte in diesem Fall sicherstellen können, dass nur korrekte und erwartete Daten in das System eingegeben werden können.

5.4. Datenvertraulichkeit (DC)

5.4.1. Sinn und Zweck

Datenvertraulichkeit stellt sicher, dass sensible Daten nur autorisierten Personen zugänglich sind. Sie schützt vor unbefugtem Zugriff und gewährleistet, dass Informationen vertraulich bleiben, sowohl während der Übertragung als auch bei der Speicherung. Dies umfasst Anforderungen wie:

Vertraulichkeit von Informationen
Die Vertraulichkeit von Informationen, die eine ausdrückliche Leseberechtigung erfordern, muss sowohl während der Übertragung als auch bei der Speicherung gewährleistet werden. Dies schliesst den Schutz vor unbefugtem Zugriff durch geeignete technische und organisatorische Massnahmen ein.

Dauerhaftigkeit von Informationen:
Komponenten, die ausser Betrieb genommen oder stillgelegt werden sollen, müssen von allen Informationen, für die eine ausdrückliche Leseberechtigung vorgesehen war, bereinigt werden. Die Löschung muss den Anforderungen entsprechender Standards und Empfehlungen genügen, um sicherzustellen, dass keine vertraulichen Daten zurückbleiben.

Verwendung von Verschlüsselung:
Falls eine Verschlüsselung erforderlich ist, müssen kryptographische Algorithmen, Schlüsselgrössen sowie Mechanismen zur Schlüsselerstellung und -verwaltung gemäss den allgemein anerkannten IT-Sicherheitsstandards und Empfehlungen verwendet werden.

- Ein Beispiel für die Kompromittierung der Datenvertraulichkeit in OT-Umgebungen ist ein unverschlüsselter Fernzugriff. Wenn Techniker oder externe Dienstleister auf OT-Systeme zugreifen, ohne Verschlüsselung zu verwenden, können sensible Betriebsdaten abgefangen und eingesehen werden.
- Ein weiteres Beispiel ist der Diebstahl von mobilen Geräten, die sensible OT-Daten enthalten. Wenn diese Geräte nicht ausreichend gesichert sind, können unbefugte Personen auf vertrauliche Informationen zugreifen.

5.4.2. *Best Practice Ansatz*

Empfehlung	Beschreibung
Netzwerksegmentierung	Sensible Daten sollten in getrennten und sicher geschützten Netzwerken gespeichert und übertragen werden. Kritische OT-Systeme sollten strikt von weniger sensiblen IT-Systemen getrennt werden.
Least Privilege-Prinzip	Zugriffsrechte so einschränken, dass nur autorisierte Personen mit minimal notwendigen Rechten Zugriff auf Daten und Systeme erhalten.
Sichere Übertragungsprotokolle	Einsatz von Sicherheitsprotokollen wie TLS/SSL (für Anwendungsebene) oder IPsec (für Netzwerkschicht), um die Vertraulichkeit und Integrität der Datenübertragung zu gewährleisten.
Zertifizierte Datenlöschverfahren	Verwendung von Standards wie ISO 27001 oder NIST 800-88, um sicherzustellen, dass sensible Daten auf ausser Betrieb genommenen Geräten vollständig gelöscht werden.
Verschlüsselungsstandards	Einsatz von AES-256 für gespeicherte Daten und TLS 1.3 für Datenübertragungen. Implementierung eines Key Management Systems (KMS) für die sichere Verwaltung und Rotation kryptografischer Schlüssel.
Regelmässige Audits und Tests	Durch Sicherheitsüberprüfungen wie Penetrationstests können Schwachstellen in Verschlüsselungsmechanismen, Netzwerken und Zugriffsrechten identifiziert und behoben werden.

Tabelle 7: Checkliste für die Gewährleistung der Systemintegrität

5.4.3. *Praxisbeispiel*

Ein aktuelles Beispiel, das die Bedeutung der Datenvertraulichkeit verdeutlicht, ist das VW-Datenleck von Dezember 2024. Eine massive IT-Sicherheitslücke, ausgelöst durch eine Fehlkonfiguration in der Software der VW-Tochterfirma cariad, hat die Standortdaten von etwa 800’000 Elektroautos der Marken Volkswagen, Audi, Seat und Skoda ungeschützt im Internet offengelegt. Dabei konnten Fahrzeugdaten mit den Namen und Kontaktdaten der Besitzer verknüpft werden. Dies ermöglichte Angreifern, Bewegungsprofile von allen Fahrzeuglenkern dieser Fahrzeuge zu erstellen. Zu 460’000 Fahrzeugen waren präzise Standortdaten einsehbar, die Rückschlüsse auf das Leben der Menschen hinter dem Lenkrad zuliessen. Die Sicherheitslücke wurde durch den Chaos Computer Club entdeckt.

Lehren aus dem Vorfall

Der Vorfall verdeutlicht, dass die Vertraulichkeit von Daten in Systemen eine entscheidende Rolle spielt, insbesondere in vernetzten Umgebungen, die sowohl IT- als auch OT-Komponenten umfassen.

Konsequenzen für Sicherheitsmassnahmen

Der Vorfall zeigt, dass die Vertraulichkeit von Daten in vernetzten Systemen nicht dem Zufall überlassen werden darf. Sicherheitsmassnahmen müssen sowohl in der Softwareentwicklung als auch im laufenden Betrieb fest verankert sein. Daraus ergeben sich folgende Konsequenzen:

- Standardisierte Sicherheitsrichtlinien, automatisierte Konfigurationsprüfungen und ein Vier-Augen-Prinzip bei Deployments sind zwingend.

- Vor jeder Inbetriebnahme sind strukturierte Sicherheitsprüfungen durchzuführen, nicht nur einmalig, sondern regelmässig und anlassbezogen.
- Personenbezogene und ortsbezogene Daten müssen standardmässig verschlüsselt gespeichert und übertragen werden. Der Grundsatz «privacy by default» ist technisch abzusichern.

Verschlüsselung bei der Übertragung und Speicherung

Die Daten der Fahrzeuge waren unverschlüsselt, wodurch sie leicht von unbefugten Dritten eingesehen werden konnten. Eine Ende-zu-Ende-Verschlüsselung hätte das Abfangen und den Missbrauch der Daten verhindert.

Sicherheitsbewusstes Softwaredesign

Der Fehler entstand durch eine Fehlkonfiguration, was auf mangelnde Sicherheitsprüfungen während der Entwicklung und Bereitstellung der Software hinweist. Regelmässige Sicherheitsaudits und Penetrationstests könnten ähnliche Schwachstellen frühzeitig aufdecken.

Zugriffsmanagement und Authentifizierung

Der unkontrollierte Zugang zu sensiblen Daten zeigt die Notwendigkeit strikter Zugriffsrechte und Mechanismen wie Multi-Faktor-Authentifizierung (MFA).

Das VW-Datenleck zeigt, wie sich mangelnde Sicherheitsmassnahmen in Systemen auf die Vertraulichkeit sensibler Daten auswirken können. Vernachlässigte Sicherheitsvorkehrungen gefährden nicht nur die Privatsphäre der Nutzer, sondern auch die Integrität und Sicherheit der zugrunde liegenden Infrastruktur. Dieser Vorfall verdeutlicht die Bedeutung einer robusten Sicherheitsstrategie, die IT- und OT-Komponenten gleichermassen schützt.

5.5. Eingeschränkter Datenfluss (RDF)

Der eingeschränkte Datenfluss (in Englisch Restricted Data Flow, RDF) ist ein grundlegendes Konzept zur Gewährleistung der IKT-Sicherheit in der Gebäudeautomation. Ziel des eingeschränkten Datenflusses ist es, den Austausch von Daten innerhalb eines Netzwerks strikt zu reglementieren, um potenzielle Angriffsvektoren zu minimieren und die Kontrolle über kritische Systeme zu maximieren. Durch eine klare Trennung und Strukturierung von Datenflüssen wird sichergestellt, dass nur autorisierte Informationen über definierte Kommunikationswege zwischen den verschiedenen Systemen und Zonen übertragen werden. Dies reduziert das Risiko, dass Cyberangriffe oder Störungen in einer Zone auf andere Bereiche übergreifen können.

Mittels Netzwerk-Segmentierung und Zonenkonzept können Datenflüsse im Netzwerk gezielt gesteuert werden. Durch diese Massnahmen lassen sich Zugriffe auf Systeme einschränken, was unnötige Datenflüsse verhindert und das Eindringen in kritische Systeme erschwert.

Eine durchdachte und sichere Netzwerkarchitektur mit logischen und physischen Segmentierungen spielt dabei eine zentrale Rolle. Insbesondere Zonenkonzepte und sogenannte Conduits ermöglichen die gezielte Kontrolle der Datenströme zwischen isolierten Systemen, was eine höhere Sicherheit und bessere Kontrollierbarkeit gewährleisteten. Ergänzt wird dieses Konzept durch den Einsatz sicherer Kommunikationstechnologien, die Datenintegrität und -vertraulichkeit auch bei der Übertragung gewährleisten.

Der NIST CSF [3] sowie der ISA/IEC 62443-Standard bieten hierfür eine umfassende Grundlage und definieren Best Practices und Vorgaben für die sichere Gestaltung und Umsetzung von Netzwerkarchitekturen, die den eingeschränkten Datenfluss gewährleisten.

Dieses Kapitel beschreibt die Massnahmen und Technologien, die notwendig sind, um den Datenfluss innerhalb der Gebäudeautomation wirksam zu reglementieren. Es adressiert sowohl physische als auch logische Segmentationen, Kommunikationsprotokolle sowie spezifische Anforderungen an die Architektur und den Betrieb der Netzwerke.

5.5.1. Netzwerkarchitektur und Netzaufteilung

Die Netzaufteilung ist eine wesentliche Methode zur Erhöhung der IT-Sicherheit, da sie die Angriffsfläche verringert und unerwünschten Netzverkehr im GA-System verhindert. Die Automatisierungssysteme müssen logisch voneinander getrennt werden, um die Sicherheit der Gebäudeautomationssysteme zu gewährleisten. Durch die Netzwerkaufteilung wird das Risiko minimiert, dass Angriffe und Bedrohungen sich von weniger sicheren zu kritischen Netzen ausbreiten.

Die logische Trennung von Netzwerken bedeutet, diese so zu konfigurieren, dass sie isoliert und unabhängig voneinander funktionieren, obwohl sie physisch verbunden sein können. Kritische Infrastrukturen und Netze werden besser geschützt, indem sie von anderen Netzen isoliert werden. Dies reduziert die Angriffsfläche und begrenzt die Auswirkungen von Sicherheitsvorfällen.

Zonenkonzepte und Conduits sind spezifische Methoden, um Netzwerke in sicherheitsrelevante Segmente (Zonen) zu unterteilen und die Kommunikation zwischen diesen Segmenten zu steuern. Zonenkonzepte nutzen logische Trennungstechniken wie VLANs und VPNs, um die Zonen virtuell zu isolieren, während Conduits diese Trennung durch kontrollierte Kommunikationskanäle unterstützen.

Abbildung 3 bildet einen Sicherheits-Netzwerk-Blueprint dar.

5.5.1.1. Zonenkonzepte

Das Zonenkonzept teilt ein Netzwerk in verschiedene Sicherheitszonen mit jeweils eigenen Anforderungen und Richtlinien. Jede Zone enthält Systeme und Geräte mit ähnlichen Sicherheitsanforderungen und wird durch strenge Sicherheitsrichtlinien und -massnahmen voneinander getrennt.

Das Zonenkonzept sollte an die spezifischen Anforderungen der jeweiligen Systeme angepasst werden, um sowohl die Sicherheit als auch die Funktionalität sicherzustellen. Bei BACnet-Systemen bspw. bedeutet dies, dass die Zonierung an die besonderen Vorgaben von BACnet angepasst werden muss, damit die Systemfunktionen uneingeschränkt erhalten bleiben.

5.5.1.2. Conduits

Conduits sind Kommunikationskanäle zwischen verschiedenen Zonen, die den Datenverkehr regeln und kontrollieren. Sie unterstützen die Umsetzung von Zonenkonzepten, indem sie den sicheren und kontrollierten Datenfluss zwischen den Zonen ermöglichen. Conduits sind ein wesentlicher Bestandteil der logischen Trennung, da sie sicherstellen, dass nur autorisierter Verkehr zwischen den Zonen fliesst.

5.5.1.3. Anwendungsempfehlung

Zonenkonzept entwickeln

Festlegen von unterschiedlichen Zonen basierend auf Risikobewertung und Sicherheitsanforderungen wie bspw.:

- DMZ (Demilitarisierte Zone): Für externe Verbindungen und Fernwartung.
- GA-Zone: Für unterschiedliche Steuerungssysteme der Gebäudeautomation, je nach IP-Konzept auch für die unterschiedlichen Gewerke.
- Bürozone: Für administrative IT-Systeme.
- Gästezone: Für Besucher und nicht vertrauenswürdige Geräte.

Festlegen von spezifischen Sicherheitsrichtlinien für jede Zone wie am Beispiel der GA-Zone:

Zugriffskontrolle:

- Nur autorisierte interne Benutzer und Geräte dürfen auf die GA-Zone zugreifen.
- Strikte Zugangskontrollen und Rollentrennung nach dem Least-Privilege-Prinzips.

Netzwerksegmentierung:

- Physische und logische Trennung von anderen Netzwerken.
- VLANs und Firewalls zur Isolierung von kritischen Systemen.

Systemhärtung:

- Regelmässige Sicherheitsupdates und Patches für alle Geräte.
- Deaktivierung unnötiger Dienste und Schnittstellen.

Überwachung und Auditing:

- Kontinuierliche Überwachung des Netzwerkverkehrs und der Systemaktivitäten.
- Regelmässige Sicherheitsüberprüfungen und Penetrationstests.

Physische Segmentierung

Physische Segmentierung bedeutet, verschiedene Teile des Netzwerks auf physisch getrennten Hardware-Komponenten (z. B. Switches und Router) zu betreiben, um ungewollte Interferenzen und Zugriffe zu verhindern.

- Wenn möglich für jede Zone separate Switches und Router einsetzten. Damit wird sichergestellt, dass ein Sicherheitsvorfall in einer Zone nicht direkt auf andere Zonen übergreifen kann.
- Wenn möglich sollen Kabelverbindungen zwischen den Geräten und verschiedenen Zonen klar definiert und dokumentiert werden, um versehentliche Verbindungen zu vermeiden.

Logische Segmentierung und Trennung

Bei der logischen Segmentierung werden VLANs und Subnetze verwendet, um innerhalb der physischen Infrastruktur unterschiedliche Netzsegmente zu schaffen und diese zu isolieren.

Es wird empfohlen einzelne VLANs für verschiedene Systemtypen und Sicherheitszonen zu konfigurieren wie am Beispiel der GA/ Produktionszone:

- Separates VLAN für HLK-Systeme
- Separates VLAN für Zutrittskontrollsysteme
- Separates VLAN für Überwachungskameras

Es wird auch empfohlen jedes VLAN in ein eigenes Subnetz zu unterteilen, um die IP-Adressierung zu verwalten und den Datenverkehr besser kontrollieren zu können.

Conduits einrichten

Es wird empfohlen, Firewalls zwischen den Zonen einzusetzen, um den Datenverkehr zu filtern und unautorisierten Zugriff zu verhindern. Es soll beispielsweise eine Firewall zwischen der DMZ und der GA-Zone eingerichtet werden.

Für den sicheren Fernzugriff auf die DMZ und die GA-Zone wird empfohlen, einen VPN-Tunnel zu konfigurieren, um die Datenintegrität und -vertraulichkeit bei externen Verbindungen zu schützen.

Zusätzlich könnte man ein Intrusion Detection und Prevention System (IDS/IPS) zwischen den Zonen implementieren, um verdächtige Aktivitäten zu überwachen und darauf zu reagieren. Dies wird jedoch in der Praxis nur selten für die Gebäudeautomation angewendet und müsste wohl eher IT übergreifend platziert werden.

Zusammenfassung

Durch diese strukturierte Vorgehensweise kann ein sicheres und effektives Gebäudeautomationsnetzwerk geschaffen werden. Die Kombination von physischen und logischen Trennungsmassnahmen mit definierten Sicherheitszonen und überwachten Conduits führt zu einer signifikanten Steigerung der OT-Security.

5.5.1.4. Netzwerk-Blueprint

Die in Abbildung 3 abgebildete schematische Darstellung zeigt einen Sicherheits-Netzwerk-Blueprint eines sicheren OT-Netzwerks und basiert auf dem gängigen Purdue-Modell.

Die oberste Ebene (blau eingerahmt) repräsentiert die Unternehmens-IT-Zone. Diese Zone umfasst geschäftskritische Systeme wie Datenbanken, Serversysteme und drahtlose Netzwerke. Sie ist vom Internet durch eine Firewall abgeschottet, um einen sicheren Zugriff zu gewährleisten. Die Verbindung zu anderen Zonen erfolgt ausschliesslich über kontrollierter Übergänge, den Conduits, die zusätzliche Sicherheitsmechanismen wie Firewalls oder Protokollfilter enthalten. Diese Zone stellt somit den Hauptzugangspunkt für externe Verbindungen dar, während gleichzeitig sichergestellt wird, dass sensible Systeme vor unbefugtem Zugriff geschützt bleiben.

Die zweitoberste Ebene der Grafik (violett eingerahmt) zeigt die demilitarisierte Zone (DMZ), die als Pufferzone zwischen der Unternehmens-IT und der GA dient. In dieser Zone befinden sich typischerweise Arbeitsstationen zur Datenanalyse, zentrale Verwaltungssysteme und Zwischenspeicher für Logdaten. Diese Zone erlaubt den Datenaustausch zwischen den industriellen und den geschäftlichen Prozessen, ohne dass eine direkte Verbindung besteht. Übergänge zwischen der DMZ und den angrenzenden Zonen sind durch zusätzliche Schutzmassnahmen abgesichert, um die Sicherheit und Integrität der Daten zu gewährleisten.

Die zweitunterste Ebene (gelb eingerahmt) stellt die GA-Zone (Prozesssteuerungszone) dar, die alle für die Automatisierung notwendigen Systeme wie Kontroller, Mensch-Maschine-Schnittstellen (HMI) und Instandhaltungsgeräte enthält. Die Kommunikation erfolgt hier primär über industrielle Ethernet-Netzwerke oder Feldbusse. Der Zugang zu dieser Zone ist streng reguliert, um sicherzustellen, dass nur autorisierte Personen oder Systeme Zugriff haben.

Die unterste Ebene (rot eingerahmt) bildet die sicherheitskritische Zone, in der Systeme untergebracht sind, die für sicherheitsrelevante Funktionen verantwortlich sind, wie beispielsweise Notabschaltungen durch FS-PLC. Diese Zone ist entweder vollständig isoliert oder über hochgesicherte Conduits mit anderen Zonen verbunden. Lokale Arbeitsstationen ermöglichen die Überwachung und Wartung dieser sicherheitskritischen Prozesse. Dabei wird durch die Minimierung der Netzwerkinfrastruktur innerhalb dieser Zone die Angriffsfläche zusätzlich reduziert.

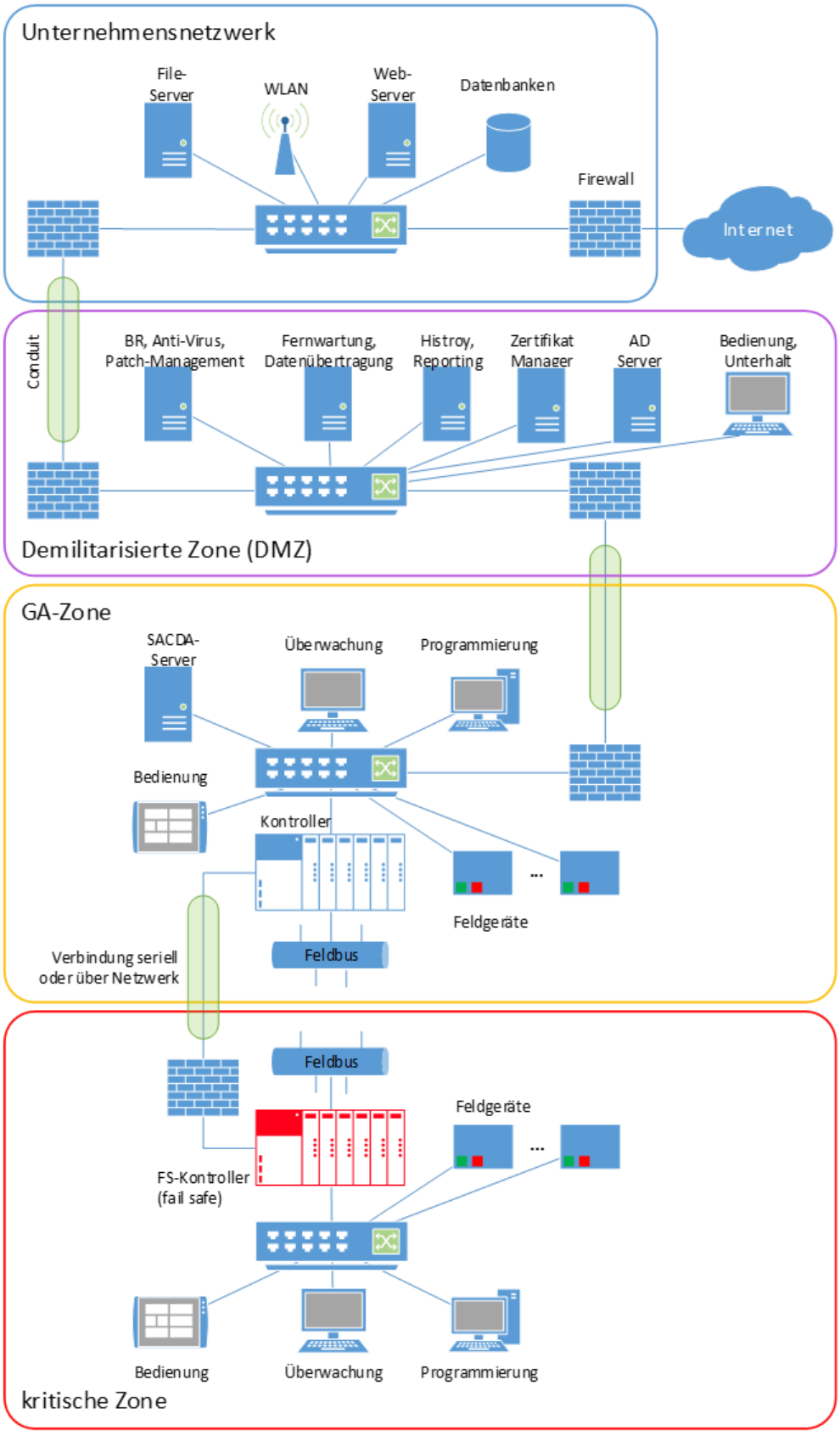

Abbildung 3: Sicherheits-Netzwerk-Blueprint

5.5.2. Kommunikationstechnologie

Zur Steuerung und Kontrolle des Kommunikationsverkehrs und somit auch des Datenflusses ist das Zusammenspiel moderner Kommunikationstechnologien von zentraler Bedeutung. In einem sicheren OT-Netzwerk kommt es darauf an, dass die eingesetzten Technologien nicht nur leistungsfähig, sondern auch robust gegenüber Sicherheitsrisiken sind.

Für die Kommunikation innerhalb der OT sind oftmals industrielle Ethernet-Protokolle wie Modbus TCP, BACnet IP oder EtherNet/IP im Einsatz. Diese Protokolle bieten Echtzeitfähigkeiten und hohe Zuverlässigkeit, jedoch müssen sie durch zusätzliche Sicherheitsmassnahmen ergänzt werden, da sie ursprünglich nicht für die heutigen Bedrohungsszenarien entwickelt wurden. Protokoll-Gateways können hier eine entscheidende Rolle spielen, um eine sichere Kommunikation zwischen unterschiedlichen Protokollen und Netzwerken zu gewährleisten.

Ein weiterer, entscheidender Faktor ist die Verwendung von Verschlüsselungstechnologien, insbesondere bei der Übertragung sensibler Daten. Technologien wie TLS (Transport Layer Security) oder IPSec ermöglichen es, Daten vor unbefugtem Zugriff zu schützen und die Integrität während der Übertragung sicherzustellen. In industriellen Umgebungen ist es zudem essenziell, dass diese Verschlüsselungstechnologien in Echtzeitumgebungen mit minimaler Latenz arbeiten können, um die Systemverfügbarkeit nicht zu beeinträchtigen.

5.5.3. Zero-Trust

Das Zero-Trust-Prinzip hat sich als zentrale Sicherheitsstrategie in der IT- und OT-Umgebung etabliert. Während herkömmliche Sicherheitsansätze üblicherweise auf einer klaren Trennung zwischen «vertrauenswürdigen internen» und «nicht vertrauenswürdigen externen» Netzwerken basieren, geht Zero-Trust davon aus, dass kein Benutzer, Gerät oder System standardmässig vertrauenswürdig ist. In einer Zero-Trust-Umgebung werden alle Zugriffe auf Systeme, Anwendungen und Daten streng kontrolliert und regelmässig überprüft.

Ein zentrales Element des Zero-Trust-Ansatzes ist die starke Authentifizierung und Autorisierung. Jeder Benutzer und jedes Gerät müssen sich eindeutig identifizieren und nachweisen, dass sie berechtigt sind, auf eine Ressource zuzugreifen. Technologien wie Multi-Faktor-Authentifizierung (MFA) und rollenbasierte Zugriffsmodelle (RBAC) sind dabei von entscheidender Bedeutung. Speziell in der GA ist es wichtig, dass ausschliesslich autorisierte Mitarbeitende, Systeme und Anwendungen Zugriff auf kritische Steuerungen erhalten.

Zero-Trust orientiert sich an etablierten Methoden, die auch in anderen Teilen dieses Dokuments erwähnt werden, etwa der kontinuierlichen Überwachung und Analyse von Aktivitäten (vgl. Kapitel 4.9) oder der Segmentierung von Netzwerken (vgl. Kapitel 5.3).

Dabei wird ein Netzwerk nicht mehr als homogene, vertrauenswürdige Zone betrachtet, sondern in kleinere, logisch getrennte Einheiten unterteilt. Die Kommunikation zwischen diesen Segmenten wird nur dann erlaubt, wenn sie explizit notwendig und autorisiert ist.

Die Umsetzung eines Zero-Trust-Ansatzes ist komplex und mit organisatorischem wie technischem Aufwand verbunden. Für Organisationen, die besonders hohe Schutzanforderungen erfüllen müssen – beispielsweise aufgrund regulatorischer Vorgaben oder der Kritikalität der betriebenen Systeme – kann dieses Modell jedoch eine sinnvolle Orientierung bieten. Für andere Organisationen können einzelne Elemente des Zero-Trust-Ansatzes selektiv übernommen werden, ohne den vollständigen Paradigmenwechsel zu vollziehen.

5.6. Zeitnahe Reaktion auf Vorfälle (TRE)

Die zeitnahe Reaktion auf Vorfälle wird durch sog. «Monitoring and Detection», auf Deutsch «Überwachung und Erkennung», Technologien gewährleistet. Grob fallen diese unter die NIST CSF-Kategorien «Detect» und «Respond». Bekannte Beispiele derartiger Technologien sind insbesondere sog. Intrusion Detection/Prevention Systems (IDS/IPS, auf Deutsch Angriffserkennungssystem bzw. Angriffsabwehrsystem), welche Vorfälle innerhalb eines Netzes erkennen und bei Bedarf auch reagieren können, sowie Endpoint Detection and Response (EDR, Endpunkt-Erkennung & -Reaktion), welche gleiches auf Endgeräte machen kann. Diese Technologien generieren dann Logs der aufgezeichneten Netzwerk-, System- und Applikationsaktivitäten, die dann konsolidiert und durch ein sogenanntes Security Incident and Events Management (SIEM, auf Deutsch Sicherheitsinformation und -eventmanagement) analysiert werden. Falls Vorfälle dann entdeckt und identifiziert werden, werden auf diese zeitnah reagiert, was auch oft durch ein sog. Security Operations Centre (SOC) koordiniert wird.

In einem OT-Umfeld wie der Gebäudeautomation sind passive Technologien (z. B. IDS) allerdings klar aktiven Technologien (z.B. IPS) vorzuziehen, da dadurch die angemessene Reaktion durch Fachexperten erfolgen kann und so die kritische Verfügbarkeit von verschiedenen Systemen nicht durch die automatische Blockierung oder Abschaltung von Systemen beeinträchtigt wird. Als Praxisbeispiel nehme man die Kühlung eines Rechenzentrums, auf die ein Hacker versucht zu zugreifen. Die passive IDS-Lösung erkennt den Vorfall und löst in der Notfallzentrale, oft im Security-Kontext das SOC, einen Alarm aus. Die zeitnahe und angemessene Reaktion darauf obliegt hier aber weiterhin den Mitarbeitenden. Eine aktive IPS-Lösung hingegen könnte hier zu Gunsten der Sicherheit die Verbindung zwischen Kühlung und restlichen Netzwerk, inklusiver zentraler Steuerung, kappen.

Eine allgemeingültige Empfehlung, welche Überwachungstechnologien und -mechanismen zu implementieren sind, gibt es aufgrund der grossen Verschiedenheit von Organisationen mit Gebäudeautomation in ihrer technischen Komplexität und ihren organisatorischen Rahmenbedingungen nicht. Stattdessen gibt es nachfolgend eine Übersicht der verschiedenen Tätigkeitsfelder, die überwacht werden können, aufgelistet mit einer groben Priorisierung nebst Kurzerläuterung in Tabelle 8.

No.	Zu überwachende Aktivität	Kurzerläuterung	Relevanz
1	Ein- und ausgehender Verkehr	Ein- und ausgehendes Netz, System und Anwendungsverkehr	Da die meisten Cyber-Angriffe das Eindringen in relevante Systeme bedingen, hat die Verkehrsüberwachung an den Schnittstellen zur Aussenwelt die höchste Wahrscheinlichkeit digitale Spuren zu identifizieren. Dies ist insbesondere nach einem Vorfall von grosser Wichtigkeit. In der GA/OT oft die einzig praktikable Methode zur Erkennung von Angriffen oder Anomalien, gerade bei nicht patchbaren Legacy-Systemen. Kann auch mit passiven Tools (z. B. Nozomi, Claroty) erfolgen.
2	Zugriff u/o Änderung kritischen Konfigurationsdaten	System & Netzwerkkonfigurationsdaten auf kritischer/administrativer Ebene	Oft unterschätzt, aber die sehr fokussierte Überwachung von Änderung an kritischen Konfigurationen erlaubt mit limitiertem Aufwand kritische Vorfälle zu erkennen. Da es meistens gewollt ist, den Status Quo bei derartigen Konfigurationen zu behalten, kann man hier auch unerlaubte Änderungsversuche proaktiv blockieren. Änderungen sind selten, dadurch hoch verdächtig. Niedriger Aufwand, hoher Nutzen.
3	Protokolle von Sicherheitstools	Antivirus (AV), Intrusion Detection/Prevention Systems (IDS/ IPS), Webfilter, Firewalls, Endpoint Detection and Response (DER)/ Extended Detection and Response (XDR)	Derartige Tools sind oft für die Bündelung durch ein SIEM ausgelegt. Hiermit sammelt man bereits erkannte Sicherheitsvorfälle oder Anomalien. Gilt vor allem für angrenzende IT-Systeme; in GA eingeschränkt verfügbar.
4	Zugangskontrolle (Access Logs)	Zugang zu Systemen, Server, Überwachungssystemen, etc.	Angriffe passieren meistens durch Einflussnahme auf Geräte, und so erlaubt die Überwachung der Zugangskontrolle auf verschiedenen Geräten sowohl vor als auch nach einem Vorfall Einblick, welche Geräte betroffen sind. Achtung, nur sinnvoll, wenn konsistente Logdaten verfügbar sind.
5	System- und Applikationslogs	Ereignisprotokoll zu System- und Netzwerkaktivitäten	Derartige Logs, oft auch Syslog genannt, können bei vielen Geräten eingeschaltet und durch Standardlösung am Markt auch eingesammelt und analysiert werden. Hierbei gibt es auch «OT-fähige» Geräte wie z.B. Nozomi, welche auch Protokolle wie BACnet verstehen können. Limitation hierbei ist eine erhöhte «Falschalarm»-Quote, welche nur durch intensives «Vorlernen» und konstante Behandlung mit dementsprechendem Aufwand zu kontern ist.

Tabelle 8: Übersicht über verschiede Überwachungstätigkeiten

Wie in Kapitel 4.4 bereits beschrieben, ist die Überwachung ein entscheidender Teil jedes Sicherheitsprogramms und verschiedene technische Massnahmen erlauben selbst Organisationen mit stark limitiertem Personal und Budget hierdurch ihre Informationssicherheit zu stärken.

5.7. Verfügbarkeit (Availability) von Ressourcen (RA)

Die verschiedenen technischen Massnahmen, die bislang beschrieben und empfohlen wurden, sind letztendlich alle Unterstützung für die Hauptanforderung an die IKT-Sicherheit der Gebäudeautomation: das Sicherstellen der kontinuierlichen und verlässlichen Verfügbarkeit aller Systeme. Eine hohe Verfügbarkeit ist essenziel für die Betriebssicherheit der Organisation, sie garantiert den Schutz von Leib und Leben und sie minimiert Ausfallzeiten und damit Kosten. Deswegen muss ein wichtiger Fokus eines Sicherheitsprogrammes sein, sich über seine konkreten Verfügbarkeitsanforderungen an seine verschiedenen Systeme und Prozesse bewusst zu sein und diese mit Massnahmen dann auch sicherzustellen.

5.7.1. Best Practice

Die drei wichtigsten technischen Massnahmen dafür sind Redundanzen, Backups und Ersatzteile. Sie alle haben zum Ziel, dass noch während oder nach einem Vorfall die Verfügbarkeit verschiedener Systeme so schnell wie möglich wiederhergestellt werden. Damit agieren diese Massnahmen als «Sicherheitspolster» oder «Fehlertoleranz» und erlauben betroffene Systeme bei einem Sicherheitsvorfall ausser Betrieb zu nehmen und sorgfältig auf Schwachstellen zu untersuchen.

Redundanzen können sowohl auf der System- als auch der Komponenten-Ebene realisiert werden. Eine Systemredundanz wäre zum Beispiel für eine wichtige Datenbank zwei Datenbankserver zu haben, welche synchronisiert sind. Wenn dann der primäre Datenbankserver ausfällt, kann ohne Datenverlust oder Ausfallzeit der sekundäre Datenbankserver genutzt werden. Da Redundanzen erhöhte Kosten bedeuten, ist es sinnvoll, nur die Systeme und Komponenten redundant aufzubauen, welche erhöhte Verfügbarkeitsanforderungen haben. Ein gutes Beispiel ist die Stromversorgung von wichtigen Kühlsystemen, für die es sinnvoll sein kann, eine Notstromversorgung als Redundanz aufzubauen.

Backups kommen mit der Perspektive der IKT-Sicherheit in zwei Arten: sogenannte Online-Backups, welche in einer Netzwerkverbindung konstant erreichbar und lesbar sind und Offline-Backups, welche keine konstante Verbindung haben. Der Unterschied ist, dass bei Offline-Backups mehr Zeit benötigt wird, die gesicherten Daten zu erhalten, diese Art von Backup aber gleichzeitig auch isolierter ist von etwaigen Cyber-Angriffen wie Ransomware. In der Gebäudeautomation lohnt es sich vor allem Backups der wichtigsten Systemkonfigurationen anzufertigen, damit bei einem Ausfall oder Vorfall diese sicher wiederhergestellt werden können.

Ersatzteile sind aufgrund der Betriebssicherheit in OT-Umfeldern wie der Gebäudeautomation schon weitverbreitet. Aber auch für die Informationssicherheit sind sie von grosser Wichtigkeit, da von Angriffen betroffene Geräte oft gar nicht vollständig von moderner Malware gesäubert werden können. Insbesondere in kritischen Einsatzszenarien wie der Gebäudeautomation ist es deswegen oft die «Best Practice», das Gerät lieber vollständig auszutauschen als ein Wiederauftreten der Malware zu riskieren.

Abschliessend haben alle drei technischen Massnahmen eins gemeinsam: ohne das regelmässige Testen hat man keine Sicherheit, dass sie im Fall eines Sicherheitsvorfall auch wie erwartet funktionieren. Ähnlich wie die Notfallpläne aus Kapitel 4.7 lohnt es sich also der Zeitaufwand für das Üben und Testen.

Praxisbeispiel

Als Praxisbeispiel nehmen wir einen Bauherren, der die Steuerung von Kühlsystemen seines Rechenzentrums als kritische Systeme identifiziert hat, bei denen eine hohe Verfügbarkeit sichergestellt werden muss. In diesem Fall lohnt es sich, die wichtigsten

Konfigurationen und Parameter der Kühlgeräte in ein Backup zu überführen. Im Falle eines Sicherheitsvorfall, in dem die Steuerung dann kompromittiert wird, kann die Steuerung schnell und sicher mit dem Backup auf die richtige Grundkonfiguration zurückgestellt werden. Dies reduziert nicht nur die Ausfalldauer, sondern verschafft der Sicherheitsorganisation auch mehr Zeit, den Sicherheitsvorfall zu beheben bevor schwerwiegendere Konsequenzen entstehen.

Änderungsverzeichnis

Version	Datum	Beschreibung
1.0	15.05.2025	Erste Vollversion nach Vernehmlassung durch KBOB