CYBERSECURITY IN DER GEBÄUDESTEUERUNGEN

Cybersecurity Planungshinweise für KNX-Systeme

Inhalt

1. Cybersicherheit für Gebäudeautomations- und -steuerungssysteme Gebäudeautomation (GA) ... 3

2. Schwachstellen von Gebäudeautomation (GA) als Risikofaktoren ... 3

3. Cybersecurity im Planungs- und Ausschreibungsprozess ... 4

3.1. Technische Gebäudeausrüstung liegt in der Verantwortung von unterschiedlichen Gewerken ... 4

3.2. Überwachung der Gebäudeautomation (GA) ... 4

3.3. Rollen- und Berechtigungsmanagement ... 5

4. IT- und OT-Netze ... 5

4.1. Cybersecurity-Anforderungen an die Gebäudeautomation (GA) ... 6

4.2. Bewertung des aktuellen Zustands ... 6

4.3. Verantwortlichkeiten und Rechenschaftspflicht für Cybersecurity ... 7

4.4. Netzsegmentierung und -Verwaltung ... 7

5. Anforderungen an die Cybersecurity von Gebäudeautomations- und -steuerungssystemen ... 8

5.1. Grundlegende Cybersecurity-Anforderungen (MUSS-Anforderungen) ... 8

5.1.1. INF.14.A1 Planung der Gebäudeautomation ... 8

5.1.2. INF.14.A2 Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA ... 11

5.1.3. INF.14.A3 Sichere Anbindung von TGA-Anlagen und GA-Systemen ... 12

5.1.4. INF.14.A4 Berücksichtigung von Gefahrenmeldeanlagen in der GA ... 13

5.1.5. INF.14.A5 Dokumentation von Gebäudeautomation (GA) ... 13

5.1.6. INF.14.A6 Separierung von Netzen der GA ... 14

5.2. Standard-Cybersecurity-Anforderungen (Sollte-Anforderungen) ... 15

5.2.1. INF.14.A7 Festlegung einer Cybersecurity-Richtlinie für die Gebäudeautomation ... 15

5.2.2. INF.14.A8 Anforderungsspezifikation für GA-Systeme ... 15

5.2.3. INF.14.A9 Entwicklung eines GA-Konzepts ... 16

5.2.4. INF.14.A10 Bildung von unabhängigen GA-Bereichen ... 17

5.2.5. INF.14.A11 Absicherung von frei zugänglichen Ports und Zugängen der GA ... 18

5.2.6. INF.14.A12 Nutzung sicherer Übertragungsprotokolle für die GA ... 18

5.2.7. INF.14.A13 Netzsegmentierung in der GA ... 18

5.2.8. INF.14.A14 Nutzung eines GA-geeigneten Zugriffschutzes ... 19

5.2.9. INF.14.A15 Absicherung von GA-spezifischen Netzen ... 19

5.2.10. INF.14.A16 Absicherung von drahtloser Kommunikation in GA-Netzen ... 20

5.2.11. INF.14.A17 Absicherung von Mobilfunkkommunikation in GA-Netzen ... 20

5.2.12. INF.14.A18 Sichere Anbindung von GA-externen Systemen 20
5.2.13. INF.14.A19 Nutzung dedizierter Adressbereiche für GA-Netze 21
5.2.14. INF.14.A20 Vermeidung von Broadcast-Kommunikation in GA-Netzen 21
5.2.15. INF.14.A21 Anzeigen der Gültigkeit von Informationen in GA-Systemen 21
5.2.16. INF.14.A22 Sicherstellung von autark funktionierenden GA-Systemen und TGA-Anlagen 22
5.2.17. INF.14.A23 Einsatz von physisch robusten Komponenten für die GA 22
5.2.18. INF.14.A24 Zeitsynchronisation für die GA 22
5.2.19. INF.14.A25 Dediziertes Monitoring in der GA 22
5.2.20. INF.14.A26 Protokollierung in der GA 22
5.2.21. INF.14.A27 Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung 23
5.3. Anforderungen für kritische Systeme mit erhöhten Anforderungen an die Cybersecurity 23
5.3.1. INF.14.A28 Physische Trennung der GA 23
5.3.2. INF.14.A29 Trennung einzelner TGA-Anlagen 23
5.3.3. INF.14.A30 Bereitstellung eines GA-eigenen Zeitservers 23

6. Schlussfolgerung: Ein störungsresistentes Gebäudeautomation (GA)-System ist auch gegen Cybersecurity-Risiken gut gewappnet. 23

Zweck des Dokuments

Dieser Leitfaden unterstreicht die Bedeutung der Cybersicherheit bei der Planung, der Implementierung und dem Betrieb von Gebäudeeinrichtungssystemen (GA) und beschreibt die damit verbundenen Sicherheitsanforderungen. Dieses Dokument konzentriert sich auf Aspekte, die für Planer, Systemintegratoren und Installateure bei der Planung und Ausführung eines KNX-Systems relevant sind.

1. Cybersicherheit für Gebäudeautomations- und -steuerungssysteme Gebäudeautomation (GA)

Die Gebäudeautomation (GA) trägt maßgeblich zur Optimierung der Gebäudeeffizienz bei, indem sie technische Prozesse wie Heizung, Lüftung, Beleuchtung und Sicherheitsfunktionen automatisiert. GA-Systeme stellen einen zentralen Bestandteil des technischen Gebäudemanagements dar. Im Zuge veränderter rechtlicher Rahmenbedingungen, neuer Risikoszenarien und eines gestiegenen Bewusstseins seitens der Kunden gewinnt die IT-Sicherheit im Gebäudemanagement zunehmend an Bedeutung.

Interne Bedrohungen können die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit jener Systeme beeinträchtigen, die für den sicheren Betrieb der Gebäudeinfrastruktur unerlässlich sind. Externe Gefahren umfassen insbesondere Sabotage, Spionage und unbefugte Zugriffe. Die Mehrzahl der Cyberangriffe richtet sich auf die Automatisierung- und Verwaltungsebenen von Gebäudesystemen; die Feldebene, beispielsweise KNX-Sensorik und -Aktoren, ist hiervon weniger betroffen. Aus diesem Grund hat die Sicherstellung der Ausfallsicherheit sowohl auf Automatisierungsebenen als auch auf Managementebene (etwa SCADA, Visualisierung sowie DDC- oder SPS-Steuerung) eine herausragende Bedeutung.

Gebäudesteuerungssysteme sind meist nicht direkt Ziel von Cyberangriffen. Stattdessen nutzen Angreifer Schwachstellen im System oder in der IT-Integration, um Zugriff auf das allgemeine Netzwerk zu erhalten.

Die Nutzung von GA kann verschiedenen Anwendergruppen einer Einrichtung offenstehen, etwa unterschiedlichen Mietern, wobei verschiedene Bereiche einer Liegenschaft jeweils über individuelle Konfigurationen verfügen können. Somit stellt Cybersecurity neben technischen Erfordernissen auch eine zentrale organisatorische Herausforderung dar.

Angesichts dieser Entwicklung ist davon auszugehen, dass die Notwendigkeit klar definierter vertraglicher Zuständigkeiten weiter steigen wird. Neue gesetzliche Vorgaben sehen vor, dass betroffene Systeme künftig von Grund auf cyber-sicher gestaltet sein müssen. Dies könnte eine Umkehr der Beweislast nach sich ziehen: Während bislang die Kunden für die Spezifikation und Kontrolle der Sicherheitsanforderungen verantwortlich sind, wird künftig erwartet, dass die Systeme standardmäßig sicher sind – es sei denn, die Kunden werden ausdrücklich auf bestimmte Ausnahmen hingewiesen und stimmen diesen zu.

2. Schwachstellen von Gebäudeautomation (GA) als Risikofaktoren

Im Bereich der Gebäudeautomation (GA) bestehen diverse Herausforderungen, die ein signifikantes Risiko für die Cybersecurity von Gebäudesteuerungssystemen und gegebenenfalls auch für angeschlossene IT-Systeme oder Drittanwendungen darstellen. Die Berücksichtigung sicherheitsrelevanter Aspekte wird häufig in der Planungsphase vernachlässigt, insbesondere wenn der zukünftige Betreiber des Gebäudes nicht feststeht. Mangelhafte Dokumentation sowie unvollständige oder fehlende Aufzeichnungen erschweren eine zuverlässige Bewertung des aktuellen Cybersecurity-Status der Gebäudesysteme erheblich. Schnittstellen zwischen Gebäudeleitsystemen und anderen technischen Systemen können sowohl absichtlich als auch unbeabsichtigt potenzielle Schwachstellen offenlegen.

Eine inadäquate Überwachung kritischer Systeme kann dazu führen, dass Ausfälle unentdeckt bleiben, wodurch das Risiko signifikanter Störungen steigt. Defizite im Rollen- und Zugriffsmanagement treten insbesondere dann auf, wenn mehrere Personen gemeinsam ein Benutzerkonto verwenden; dies beeinträchtigt die Nachverfolgbarkeit von Aktivitäten und erschwert die Sicherstellung der Verantwortlichkeit. Da Gebäudesysteme oftmals über lange Lebenszyklen – häufig über mehrere Jahrzehnte – betrieben werden, ist eine strategische und vorausschauende Planung erforderlich, um deren Sicherheit langfristig gewährleisten zu können.

Integratoren und Lieferanten von Gebäudesteuerungssystemen sind zunehmend gefordert, zusätzliche Verantwortlichkeiten zu übernehmen, insbesondere hinsichtlich der Bereitstellung von Software-Updates zur Behebung identifizierter Schwachstellen. Im Kontext des Cyber-Security-Resilience-Act der Europäischen Union gilt die umgekehrte Beweislast: Kunden, die eine Schwachstelle ausnutzen, können geltend machen, sie seien davon ausgegangen, dass das System sicher und konform mit gesetzlichen Vorgaben sei. Infolgedessen obliegt es Herstellern, Lieferanten, Installateuren und Integratoren, nachzuweisen, dass die Produkte dem Stand der Technik entsprechen, ordnungsgemäß installiert wurden sowie sämtliche Sicherheitsausnahmen transparent kommuniziert und vom Kunden genehmigt wurden.

3. Cybersecurity im Planungs- und Ausschreibungsprozess

Während der Bauphase sind Mieter und Endnutzer häufig noch nicht bekannt. Die Anforderungen an das Gebäudeleit-System werden daher erst nachträglich gemäß den Bedürfnissen der Nutzer definiert. Gegebenenfalls bedarf das System einer Anpassung an geltende Cybersecurity-Standards.

Systemplaner und Lieferanten sollten weiterhin flexibel auf notwendige Änderungen nach Bezug des Gebäudes reagieren. Eine unzureichende Planung kann dazu führen, dass die Dokumentation lückenhaft ist, wodurch zukünftige Aktualisierungen kostenintensiv und aufwendig werden können. Für eine ordnungsgemäße Umsetzung von Änderungen benötigen Systemintegratoren umfassende und genaue Bestandsunterlagen. Präzise Spezifikationen sowie eine sorgfältige Dokumentation erleichtern zudem die Bewertung, ob Anpassungen auf bestehende Mängel oder kostenpflichtige Abweichungen zurückzuführen sind.

3.1. Technische Gebäudeausrüstung liegt in der Verantwortung von unterschiedlichen Gewerken

Die Gebäudeleittechnik und das technische Gebäudemanagement agieren häufig in voneinander abgegrenzten Gewerken. Dies kann im Falle von Systemausfällen zu Verzögerungen führen, da Verantwortlichkeiten sowie Kontaktdaten oder Service Level Agreements nicht eindeutig festgelegt sind. In der Folge steigen die Kosten für die Fehlerbehebung. Die interdisziplinäre Zusammenarbeit mit anderen Branchen stellt sowohl technisch als auch vertraglich eine Herausforderung dar.

Cybersecurity-Risiken an Schnittstellen zwischen Gewerke-Teilsystemen werden häufig unterschätzt, insbesondere wenn klare vertragliche Regelungen fehlen. Angesichts der steigenden Erwartungen, dass Systeme standardmäßig mit Cyber-Security-Maßnahmen ausgestattet sind, ist bei der Integration von Drittanbietersystemen besondere Sorgfalt erforderlich. Dies gilt insbesondere für ältere Anlagen, deren Sicherheitsstandards oftmals nicht mehr dem aktuellen Stand entsprechen. Zur Risikominderung werden üblicherweise Firewalls, Edge-Geräte oder Proxys eingesetzt. Werden Schnittstellen jedoch nicht eindeutig spezifiziert und sicherheitsrelevante Aspekte nicht ausreichend berücksichtigt, besteht das Risiko, dass die Kosten zur Behebung potenzieller Schwachstellen vertraglich nicht geregelt sind.

Systemänderungen werden häufig erst in späten Projektphasen erforderlich oder beantragt. Eine sorgfältige Dokumentation unterstützt die effiziente Umsetzung dieser Änderungen und trägt dazu bei, vermeidbare Kosten zu minimieren. Eine präzise Dokumentation ermöglicht zudem eine klare Unterscheidung zwischen Änderungen zur Fehlerbehebung und solchen, die zur Einhaltung von Vertragsanforderungen oder genehmigten Anpassungen notwendig sind.

3.2. Überwachung der Gebäudeautomation (GA)

Gebäudeautomation (GA) und Technische Gebäudeausrüstung (TGA) umfassen Sensoren, Aktoren, Steuerungen und häufig auch ein Überwachungs- oder Visualisierungssystem. Ohne angemessene Überwachung können Störungen und Sicherheitsverletzungen unbemerkt bleiben. Es ist wichtig, eine Überwachungsstrategie zu entwickeln, die einen effizienten Betrieb gewährleistet, den Systemzugang verwaltet und Änderungen aufzeichnet.

Diese Anforderung betrifft oft mehrere Parteien. Feldgeräte oder Ursprungsdaten können Teil von Subsystemen wie einer KNX-Linie sein, während übergeordnete Gebäudeautomationsdienste wie Trendprotokolle oder Fehlerbenachrichtigungen vom Überwachungs- oder Visualisierungssystem übernommen werden. Teilen Sie die Aufgaben klar auf und weisen Sie die zu erbringenden Leistungen bestimmten Verträgen zu.

3.3. Rollen- und Berechtigungsmanagement

Für zentrale Anwendungen der Gebäudeautomation wie Supervisory Control and Data Acquisition (SCADA) ist ein System zur Verwaltung von Benutzeridentitäten und Zugangsrechten erforderlich. Ein fehlerhaftes Design oder eine unzureichende Implementierung kann zu Schwierigkeiten führen, etwa durch gemeinsam genutzte Logins oder den fortbestehenden Zugang ehemaliger Mitarbeiter, was das Risiko unbefugten Zugriffs erhöht. Es empfiehlt sich, die Zugangsverwaltung frühzeitig zu planen und die Nutzerrechte regelmäßig zu überwachen.

Auch Inbetriebnahme-Instrumente wie ETS sollten entsprechend behandelt werden. Diese Tools verfügen jedoch häufig nicht über rollenbasierte Zugriffskontrollen und sichern oft lediglich eine lokale Datenbank mit einem Passwort. Dadurch ist ein Zugriff auf die Anlage für jede Person möglich, die eine Kopie des ETS-Projekts besitzt, selbst wenn das ETS-Passwort nach der Übergabe geändert wurde. Systemlieferanten und Integratoren sollten Dokumentationen über alle Personen führen, die auf Projektierungsdatenbanken zugreifen, und die Sicherheitsrichtlinien mit dem Kunden abzustimmen.

4. IT- und OT-Netze

Die Cybersecurity im Bereich der Gebäudeautomation (GA) umfasst Akteure aus den Bereichen IT und Gebäudesteuerung, die jeweils unterschiedliche Schwerpunkte bezüglich Sicherheit und Betrieb setzen. Das Verständnis dieser verschiedenen Perspektiven trägt dazu bei, Missverständnisse zu vermeiden.IT-Netzwerke (Informationstechnologie) und OT-Netzwerke (Betriebstechnik, einschließlich Gebäudesteuerung und technischer Gebäudeausstattung) unterscheiden sich hinsichtlich ihres Zwecks, ihrer Umgebung und ihrer Prioritäten. Nachfolgend ist ein Vergleich aufgeführt:

IT (Informationstechnologie)-Netze

- Zweck: Verwalten Sie Daten, Kommunikation und Geschäftsprozesse.
- Umwelt: Büroräume, Rechenzentren, Cloud-Infrastruktur.
- Beispiele sind E-Mail-Systeme, ERP-Software, Datenbanken und Websites.
- Prioritäten:
    1. Vertraulichkeit (Schutz der Daten vor unberechtigtem Zugriff)
    2. Integrität (Sicherstellung der Richtigkeit und Unverfälschtheit der Daten)
    3. Verfügbarkeit (Systeme sind einsatzbereit und laufen)

OT (Operational Technology) Netzwerke

- Zweck: Überwachung und Steuerung physischer Geräte und Prozesse.
- Umwelt: Industrielle Umgebungen wie Fabriken, Kraftwerke und Gebäudeautomation.
- Beispiele hierfür sind speicherprogrammierbare Steuerungen (PLCs), SCADA-Systeme, Sensoren und Aktoren.
- Prioritäten:
    1. Verfügbarkeit (Systeme müssen kontinuierlich laufen)
    2. Sicherheit (Vermeidung von Schäden an Menschen und Geräten)
    3. Integrität (genaue Kontrolle der physischen Prozesse)

Die Beteiligten aus der IT und der Gebäudesteuerung verfolgen unterschiedliche Ziele. Es ist wichtig, Anforderungen, Cybersecurity-Aspekte und Prioritäten klar abzustimmen. Für jede Anforderung sollte eine Hauptverantwortliche Person benannt werden; weitere Beteiligte oder Zuliefernde können miteinbezogen werden, wobei die Verantwortung eindeutig geregelt sein muss.

Die Kommunikation zwischen den IT-Abteilungen und dem Systemintegrator für Gebäudeautomation (GA) trägt dazu bei, die Sicherheit des Systems sicherzustellen. Häufig verwaltet die IT-Abteilung sowohl das OT- als auch das IT-Netzwerk, insbesondere wenn das OT-Netz ein VLAN und kein physisch getrenntes LAN ist.

KNX-Systemintegratoren sollten berücksichtigen, dass KNX-Multicast-IP-Kommunikation (KNXnet/IP Routing) nutzt, während IT-Fachkräfte diese Technologie oftmals vermeiden möchten. Eine frühzeitige Abstimmung mit der IT-Abteilung hilft, potenzielle Herausforderungen zu identifizieren und Anforderungen zu klären.

Es ist erforderlich, nicht nur das GA-System gegen Angriffe abzusichern, sondern auch sicherzustellen, dass die IT-Konfigurationen, welche die Kommunikation der GA-IP-Geräte ermöglichen, keine Schwachstellen enthalten, die einen unerwünschten Zugriff auf das Netzwerk erlauben.

4.1. Cybersecurity-Anforderungen an die Gebäudeautomation (GA)

Die Festlegung grundlegender Sicherheitsprinzipien ist ein entscheidender Schritt bei der Erstellung von Anforderungsspezifikationen für Gebäudeautomation (GA). Dabei empfiehlt es sich, etablierte Ressourcen wie **AMEV,** VDMA 24774 sowie das **BSI IT-Grundschutz** Kompendium als Orientierungshilfen heranzuziehen.

Obwohl diese Leitfäden und Vorschriften primär auf den deutschen Markt zugeschnitten sind, beruhen sie auf international anerkannten IT-Standards und -Best Practices und dienen daher auch außerhalb Deutschlands als wertvolle Referenz. Die genannten Dokumente thematisieren relevante Aspekte der IT-Sicherheit:

- Gebäudeautomationsnetzwerke (Schnittstellen, Fernwartung, etc.)
- Härtung von Komponenten der Gebäudeautomation (Dienste, Konten, Verschlüsselung)
- Passwortrichtlinien (Komplexität, Ablauf, fehlgeschlagene Versuche, automatische Abmeldung, Verlauf)
- Updates, Upgrades und Wartung (Hardware, interne/externe Laptops, Schnittstellen)
- Protokollierung (Benutzeraktionen, Datenänderungen, Umschaltungen und Konfigurationsaktionen unter Beachtung der Datenschutzgesetze)

Um Cybersecurity-Risiken zu minimieren, sollten bei der Planung eines Gebäudeautomationssystems stets die folgenden Grundsätze berücksichtigt werden:

- IT-Sicherheit von Anfang an.
- Gewährleistung einer gründlichen Dokumentation und der Transparenz des Systems.
- Entwerfen Sie sichere Schnittstellen und berücksichtigen Sie Zugangskontrollen für zentrale und kritische Gebäudeautomation (GA)-Komponenten.
- Planen Sie die laufende Systemwartung und -aktualisierung, um eine optimale Leistung zu gewährleisten.

Viele Cybersecurity-Anforderungen betreffen sowohl TGA als auch GA-Systeme und werden oft von unterschiedlichen Anbietern vertraglich umgesetzt. Es ist entscheidend, Zuständigkeiten klar zuzuweisen und die Einhaltung der Verträge zu prüfen.

4.2. Bewertung des aktuellen Zustands

Beginnen Sie mit der Bewertung der Cybersecurity bestehender Geräte, Anlagen oder bestimmter Technologien. Gehen Sie nicht davon aus, dass Geräte ohne Überprüfung sicher sind. Die Segmentierung des Netzes ist für eine angemessene Sicherheit notwendig. Wurde dies berücksichtigt?

- Welche Cybersecurity-Eigenschaften bietet die vorhandene oder spezifizierte Ausrüstung?
- Unterstützt das Gerät sichere Kommunikationsprotokolle, wie KNX Secure, BACnet/SC oder OPC UA?
- Wurden die vorhandenen Geräte so konfiguriert, dass sie verschlüsselte Kommunikation verwenden?
- Schreibt die Spezifikation ausdrücklich vor, dass sichere Geräte so in Betrieb genommen werden müssen, dass sie nach Möglichkeit über sichere Protokolle kommunizieren?
- Falls proprietäre Kommunikationsprotokolle verwendet werden, ist die Kommunikation verschlüsselt, oder verlässt sich der Anbieter auf "Security by Obscurity"?
- Kann bei nicht verschlüsselter Kommunikation ein ausreichendes Sicherheitsniveau durch Netzsegmentierung und IT-Sicherheit erreicht werden?

- Sind genügend Informationen verfügbar, um sicherzustellen, dass das System den Sicherheitsanforderungen und -richtlinien des Kunden entspricht?
- Wer wird die IT-Infrastruktur des OT-Netzes und seine Komponenten bereitstellen und warten?
- Wie erfolgt die Übergabe von Passwörtern, Sicherheitsschlüsseln oder Zertifikaten?
- Wie wird überwacht, wer Zugriff auf das Passwort, die Projektdaten oder sogar das System selbst hat?

Systemlieferanten und -integratoren werden dazu angehalten, möglichst präzise Informationen bereitzustellen. Falls bestimmte Daten nicht verfügbar sind oder wenn einzelne Geräte keinen Schutz gegen Cyberangriffe bieten, sollte dies entsprechend dokumentiert werden. Für die endgültige Auswahl bildet die Bewertung die Grundlage; alle relevanten Informationen sind darzulegen und fehlende Angaben zu vermerken, um einen transparenten Entscheidungsprozess zu ermöglichen..

4.3. Verantwortlichkeiten und Rechenschaftspflicht für Cybersecurity

Für jedes verwaltete System oder jede Gruppe sollte klar definiert und dokumentiert werden, wer für Verantwortung und Rechenschaftspflicht zuständig ist. In bestimmten Fällen kann es notwendig sein, Aufgaben weiter zu präzisieren. Verantwortlichkeit und Rechenschaftspflicht können voneinander abweichen; beispielsweise berichtet die verantwortliche Person, wie ein Systemintegrator, regelmäßig an die rechenschaftspflichtige Person, oft der Auftragnehmer. Eine strukturierte Kommunikation unterstützt die Entscheidungsfindung und trägt zu effektivem Risikomanagement bei, insbesondere wenn mehrere Parteien – etwa Gebäudeeigentümer, Mieter oder Organisationen – eingebunden sind.

Die Begriffe „Verantwortung“ und „Rechenschaftspflicht“ werden oft gemeinsam verwendet, weisen jedoch insbesondere im Kontext von Management und Organisation unterschiedliche Bedeutungen auf. Hier ist eine einfache Aufschlüsselung:

Verantwortung

Definition: Ausführung einer Aufgabe oder Pflicht.

Schwerpunkt: Aktion - was jemand tun soll.

Beispiel: Ein Techniker ist für die Wartung der Klimaanlage zuständig.

Die Verantwortung bezieht sich auf den Teil des "Handelns". Der Systemintegrator für Gebäudeleittechnik erfüllt in der Regel diese Aufgabe.

Rechenschaftspflicht

Definition: Verantwortlich sein für das Ergebnis einer Aufgabe oder Entscheidung.

Schwerpunkt: Eigentümerschaft - Die Partei, die haftbar ist, wenn etwas schief geht.

Beispiel: Der Systemintegrator trägt die Verantwortung für das einwandfreie Funktionieren der Gebäudesysteme. Rechenschaftspflicht bezeichnet die Verantwortlichkeit für das erzielte Ergebnis und bezieht sich üblicherweise auf die vertraglich verpflichtete Partei, häufig den Mechanik- oder Elektroinstallateur im Be-reich der Gebäudeautomation.

Die Festlegung des KNX-Systemintegrators als verantwortliche Instanz erfolgt gemäß den jeweiligen vertraglichen Vereinbarungen. Wird beispielsweise die KNX-Anlage vom Elektroinstallateur an den Kunden geliefert und die Inbetriebnahme an den Systemintegrator delegiert, liegt die Hauptverantwortung und Haftung beim ausführenden Unternehmer. In diesem Fall obliegt dem Systemintegrator eine abgeleitete Verantwortung gegenüber dem Auftragnehmer.

4.4. Netzsegmentierung und -Verwaltung

Eine Sicherheitsstrategie für die Planung der Gebäudeautomation (GA) berücksichtigt Schutzmaßnahmen wie Datenabsicherungen, Firewalls sowie z.B. auch unterbrechungsfreie Stromversorgungen. Die Anforderungen an die Benutzerfreundlichkeit werden entsprechend dem jeweiligen Betriebskonzept festgelegt. Ziel ist ein ganzheitlicher Schutz des gesamten Gebäudesystems und der integrierten Systeme.

Die Zielsetzungen sind bereits in der Planungsphase als Teil einer umfassenden Sicherheitsstrategie für die Betriebs-Technologie (OT) zu definieren, welche Maßnahmen zur Einbindung aller OT-Komponenten umfasst. Zuständigkeiten werden Zulieferern, Systemintegratoren und dem Gebäudebetreiber zugewiesen. In die Sicherheitsstrategie für Gebäudeautomationssysteme sind folgende Elemente einzubeziehen:

- **OT-Architektur:** Festlegung der Struktur und Komponenten des betrieblichen Technologieumfelds.
- **Netzgestaltung und Segmentierung:** Planung der Netzstruktur mit Unterteilung in sichere Zonen zur Begrenzung des Zugangs und Reduzierung von Risiken.
- **Patch-Verwaltung:** Regelmäßige Aktualisierung aller Systeme und Geräte mit Sicherheits-Patches.
- **Inventarverwaltung:** Pflege eines aktuellen Inventars sämtlicher Hardware- und Softwarekomponenten des Systems.
- **Notfallmanagement:** Umsetzung von Backup-Lösungen und Redundanzstrategien zur Aufrechterhaltung des Betriebs bei IT-Netzwerkausfällen oder -Vorfallen.
- **Risikobewertung und Schutzbedarf:** Identifikation potenzieller Risiken sowie Festlegung des erforderlichen Schutzniveaus für jede Komponente.
- **Empfehlungen zur Personalausstattung:** Hinweise auf Anzahl und Qualifikation des Personals, das für einen sicheren Betrieb und die Wartung des Systems notwendig ist. Es ist erforderlich, dass die Mitarbeitenden die spezifischen IT-Anforderungen von Gebäudeleitsystemen kennen.

Für Netzsegmentierung und Asset Management sollten die nativen Segmentierungstechniken der Gebäudeautomations-Protokolle z.B. wie von KNX und BACnet eingesetzt werden. Ein fehlertolerantes Gebäudeautomationssystem, das Fehler in bestimmten Bereichen berücksichtigt, trägt zur Erhöhung der Robustheit und Widerstandsfähigkeit bei Cyber-Security-Vorfällen bei. Um Ausfallsicherheit und Robustheit der Gebäudeautomation (GA) zu stärken, empfiehlt es sich, Steuerungsfunktionen möglichst lokal zu implementieren, beispielsweise bei einem KNX-System idealerweise innerhalb einer KNX-TP-Linie.

Installieren Sie systematisch Sicherheitspatches und -updates und überprüfen Sie anschließend die Systemfunktionalität, wofür möglicherweise Inbetriebnahme-Tools erforderlich sind. Es ist wichtig zu prüfen, ob diese Tools öffentlich zugänglich, kostenlos oder kostenpflichtig sind oder ob eine kommerzielle Vereinbarung mit dem Anbieter erforderlich ist. Jeder kann das KNX-Inbetriebnahme-Tool ETS bei der KNX-Assoziation erwerben.

5. Anforderungen an die Cybersecurity von Gebäudeautomations- und -steuerungssystemen

Die folgenden Anforderungen basieren auf dem **IT-Grundschutz-Baustein INF.14** Gebäudeautomation des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dieser Leitfaden bietet Empfehlungen und Hinweise für Behörden, Unternehmen und Institutionen zum Schutz von Daten, Systemen und Informationen.

Das BSI verfolgt einen Ansatz für Informationssicherheit, der technische, infrastrukturelle, organisatorische und personelle Aspekte einbezieht. Diese Herangehensweise ermöglicht eine systematische Identifikation und Umsetzung relevanter Sicherheitsmaßnahmen. Der Leitfaden findet offiziell nur Anwendung in Deutschland; seine Methoden orientieren sich jedoch an etablierten Standards der IT-Sicherheit und können auch außerhalb Deutschlands genutzt werden, ohne rechtliche Verbindlichkeit zu besitzen.

5.1. Grundlegende Cybersecurity-Anforderungen (MUSS-Anforderungen)

Diese grundlegenden Anforderungen sollten immer angewendet werden.

5.1.1. INF.14.A1 Planung der Gebäudeautomation

Im Rahmen der Gebäudeautomation (GA) sind Anforderungen an die Cybersecurity konsequent in den Entwurfs- und Entwicklungsprozess zu integrieren. Der Systementwurf sollte sämtliche GA-Steuerungen, einschließlich HVAC, Beleuchtung, Beschattung sowie Energiemanagement, unter Berücksichtigung bewährter Sicherheitskonzepte, standardisierter Systeme und Protokolle umfassen. Die regelmäßige Aktualisierung von Spezifikationen und technischen Zeichnungen ist hierbei essenziell.

Definition und Auswahl von Technologien

- Anzuschließende Anlagen und Geräte.
- Verdrahtung, Produktverfügbarkeit und Kundenbedürfnisse.
- Erforderliche Verbindungs- und Kommunikationstechnologien.
- Gewährleistung der Übereinstimmung mit den rechtlichen und sicherheitstechnischen Anforderungen.

Optimierung des Einsatzes von Gebäudeautomation (GA)-Technologien

Es wird empfohlen, Sicherheitsrichtlinien einzuhalten, indem standardisierte Kommunikationsprotokolle verwendet werden. Von proprietären Protokollen, denen es an aktuellen Sicherheitsstandards fehlt, sollte abgesehen werden.

Vermeidung unerwünschter Interaktionen und Abhängigkeiten innerhalb der Gebäudeautomatisierung.

Jedes System sollte so konzipiert sein, dass Fehler oder Störungen keinen Einfluss auf andere Teile der Anlage haben. Beispielsweise ermöglichen KNX-Segmente eine logische und galvanische Trennung einzelner Systeme.

Darüber hinaus ist zu prüfen, inwieweit Geräte und GA-Dienste von einer kontinuierlichen Verfügbarkeit externer Cloud-Dienste abhängig sind. Dienstanbieter sollten in der Lage sein, flexibel auf Änderungen bei Internet- oder Cloud-Anbietern zu reagieren. So sollten sie beispielsweise eine „Opt-Out-Option“ anbieten, die eine eingeschränkte Funktionsfähigkeit für Kunden ermöglicht, die die Cloud-Dienste nicht weiter in Anspruch nehmen möchten, die aber dennoch die Anlage lokal weiter betreiben müssen. Für TGA- und GA-Anlagen müssen eindeutig festgelegte Offline-Funktionen stets sichergestellt sein.

Focus Aspekte der detaillierten Planung

Die sichere gebäudeübergreifende Vernetzung umfasst:

- Internet, WAN, LAN, WLAN, drahtlose Netzwerke und Feldbusse
- Sichere Kommunikationsprotokolle
- Zugriffsschutz für zentrale Steuerungskomponenten
- Sicherung der offenen Schnittstellen
- Sichere Integration von externen Systemen, wie z.B. Facility Management
- Schutz und Protokollierung von Fernwartungszugängen
- Sichere IP-Kommunikation in Gebäudeautomation-VLAN-Netzen
- Segmentierung des Gebäudeautomation-Netzes

Verwendung des Internet-Protokolls (IP)

Viele Gebäudeautomationsprotokolle, wie KNXnet/IP, BACnet/IP oder Modbus TCP, basieren auf IP (IPv4 und IPv6).

- Die Adressbereiche müssen skalierbar und gut strukturiert sein.
- Planen Sie IP-Mechanismen wie Broadcast und Multicast sorgfältig, um Netzwerkprobleme zu vermeiden.

Schutz der Schnittstellen

Schutzmaßnahmen an Gateways und Routern zu Subsystemen, Geräten, anderen GA-Systemen sowie Fern- oder Cloud-Diensten sind zentral für die Planung der Gebäudeautomation. Dies ist besonders wichtig, wenn:

- Die Gebäudeautomation (GA) unabhängig und unbeeinflusst von anderen Teilsystemen oder Segmenten funktionieren muss (siehe INF.14.A22).
- Erforderliche Teilsysteme können aufgrund technischer Einschränkungen nicht oder nur teilweise sicher in Gebäudeautomation (GA) integriert werden (siehe INF.14.A3).

In der Planung müssen die Komponenten und Mechanismen der Cybersecurity detailliert beschrieben werden, wie z. B.:

- Sicherheitsmethoden, die das Gebäudeautomation System nativ unterstützt.
- Firewalls zum Schutz von Teilsystemen oder Segmenten

Während der Detailplanungsphase sind sämtliche für ein sicheres Gebäudeautomationssystem erforderlichen Parameter festzulegen. Darüber hinaus sollten spezifische Konfigurationsrichtlinien klar definiert werden.

Einführungsplanung für Gebäudeautomation (GA)

In der Ausführungsplanung wird dargelegt, wie die Detailplanung durchgeführt werden soll. Sie umfasst:

- Angabe der erforderlichen Schritte.
- Festlegung der Reihenfolge, der Zuständigkeiten und des Zeitplans.

Bei der Endabnahme wird überprüft, ob die Umsetzung mit dem Plan übereinstimmt und alle Anforderungen erfüllt sind. Abweichungen werden dem Planungsteam gemeldet. Die Wechselwirkungen und Abhängigkeiten zwischen Geräten, individuellen Steuer- und Bussystemen der Gewerke und Gebäudeautomation (GA) müssen dokumentiert werden.

Die Inbetriebnahme der GA ist sorgfältig zu planen (siehe INF.14.M2). Der Implementierungsplan muss auch die notwendigen Tests für die Inbetriebnahme der GA enthalten.

Betriebliche Sicherheitsplanung für Gebäudeautomations- und -steuerungssysteme

(Gebäudeautomation (GA)

Nach Abschluss der Detail- und Ausführungsplanung ist der nächste Schritt die Planung des sicheren Betriebs des Gebäudeautomationssystems. Dazu gehören mindestens die folgenden Angaben:

- Sicherheitsmaßnahmen für Gebäudeautomation (GA)-Verwaltungssysteme
  (siehe INF.14.M12 - sichere Kommunikationsprotokolle, INF.14.M13 - Netzsegmentierung, INF.14.M14 - Zugriffsschutz)
- Ein Rollen- und Berechtigungsmodell zur Kontrolle, wer auf was zugreifen darf
- Verwaltung der Konfigurationsdateien der Gebäudeautomation (GA) und deren Komponenten
- Integration von Gebäudeautomation (GA)-Komponenten in Überwachungs-, Alarmierungs- und Protokollierungssysteme
  (siehe INF.14.M25 - Spezielle Überwachung, INF.14.M26 - Protokollierung in Gebäudeautomation (GA))
- Ein Backup-System für Gebäudeautomation (GA) oder eine Verbindung zu einer zentralen Backup-Lösung

Überlegungen zur Personalausstattung und Verfügbarkeit

Da Gebäudeautomations- und Steuerungssysteme häufig rund um die Uhr verfügbar sein müssen, ist es wichtig, für Situationen zu planen, in denen geschultes Personal nicht vor Ort sein kann. Dies bedeutet:

- Entweder Anpassung der Verfahren an die Fähigkeiten der verfügbaren Mitarbeiter
- oder die Schulung von Mitarbeitern, damit sie bei Bedarf dringende Aufgaben erledigen können
  (siehe INF.14.M27 - Berücksichtigung von Wechselwirkungen zwischen Gebäudeautomation (GA)-Komponenten in der Notfallplanung)

Laufende Überprüfungen und Compliance-Checks

Zur Aufrechterhaltung oder Verbesserung der Informationssicherheit:

- Regelmäßige Überprüfung aller Planungsunterlagen und Konzepte
- Vergleich des geplanten mit dem tatsächlichen Systemzustand
- Prüfen, ob die Systeme gemäß den Spezifikationen konfiguriert sind
- Alle Befunde klar dokumentieren
- Abweichungen begründen oder sofort beheben

Es ist notwendig, die Anforderungen in einzelne Komponenten aufzuschlüsseln, die mit konkreten Handelsverträgen verknüpft werden können. Neben der Spezifikation der zu erbringenden Leistungen und der geforderten Sicherheitseigenschaften ist es auch wichtig, alle bekannten Einschränkungen und vereinbarten Abweichungen von den festgelegten Sicherheitsrichtlinien zu dokumentieren. So kann es beispielsweise sein, dass bestimmte Feldgeräte ohne Verschlüsselung kommunizieren müssen, und eine Risikobewertung könnte ergeben, dass dies nur ein minimales Risiko darstellt. Nach den EU-Cybersecurity-Vorschriften, wie dem Cybersecurity Resilience Act, ist dies zulässig, sofern der Anbieter nachweisen kann, dass der Kunde ausdrücklich informiert wurde und beide Parteien zugestimmt haben.

5.1.2. INF.14.A2 Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA

Eine wirksame Koordinierung von technischen und Gebäudeautomation (GA) ist für einen reibungslosen Gebäudebetrieb unerlässlich. Es müssen klar definierte Schnittstellen zwischen den Teams eingerichtet und dokumentiert werden, die regelmäßig überprüft und aktualisiert werden, um die Effektivität und Effizienz aufrechtzuerhalten. Alle Änderungen sollten sich in aktualisierten Definitionen niederschlagen. Diese Dokumentation muss alle Sicherheitsmaßnahmen für die Gebäudeleittechnik und das technische Gebäudemanagement enthalten. Es sollte übersichtlich und leicht verständlich sein und die Anforderungen und Spezifikationen für sichere Abläufe explizit darlegen. Spezifische Sicherheitsmaßnahmen für jeden Handelsbereich sollten mit dem allgemeinen Sicherheitsrahmen in Einklang stehen.

Management der Auftragsvergabe

Das Inbetriebnahme Management gewährleistet, dass ein Gebäude wie vorgesehen funktioniert und die Betriebsanforderungen erfüllt. Seine Hauptaufgabe besteht darin, die verschiedenen Gewerke und Beteiligten in allen Projektphasen und während der ersten Nutzung des Gebäudes zu koordinieren. Da zahlreiche Gewerke und Komponenten beteiligt sind, muss die Inbetriebnahme gewerkeübergreifend geplant werden und sollte frühzeitig in die Gebäudeplanung einbezogen werden. Bei der Inbetriebnahme müssen auch die verschiedenen Funktionen berücksichtigt werden, die mit der Gebäudeautomation interagieren, wie z. B.:

- Gebäudenutzer oder Mieter
- Interne oder externe Betreiber (z. B. Gebäudemanagement), die Gebäudeautomation (GA) und zugehörige Gewerksteilsystemen verwalten und warten, z. B. Beleuchtungssteuerung, HLK-Steuerung oder Energieüberwachung und -verwaltung.
- Externe Dienstleister, die für Wartungsarbeiten Zugang benötigen
- Facility Manager für Verwaltungsaufgaben und Kostenoptimierung
- Systemadministratoren die für Backups, Systemeinstellungen und Support zuständig sind.
- Installateure und Integratoren, die Hardware, Software oder Firmware aktualisieren

Eine Person kann mehrere Rollen übernehmen, oder eine Rolle kann von mehreren Gruppen besetzt werden (wie verschiedene Mieter in einem Gebäude).

Das Inbetriebnahme Management muss auch die Abhängigkeiten und Wechselwirkungen zwischen GA-Komponenten und Gebäudesystemen der individuellen Gewerke berücksichtigen. So sollte beispielsweise die Reihenfolge, in der die Systeme in Betrieb genommen werden, festgelegt und koordiniert werden. Zu den wichtigsten zu definierenden Punkten gehören:

- Die Reihenfolge der Inbetriebnahme von Gebäudesystemen
- Die Reihenfolge der Anbindung von Teilsystemen der individuellen Gewerke und TGA-Anwendungen an eine übergeordnete Gebäudeautomation (GA)
- Das Verfahren zur Verbindung von Gebäudeautomation (GA) mit anderen Systemen (z. B. technisches Management)

Es sollten Kontrollpunkte festgelegt werden, um sicherzustellen, dass jeder Schritt abgeschlossen ist, bevor der nächste Schritt beginnt. Nach der Installation und der ersten Inbetriebnahme sollten die Sicherheitseinstellungen für die Betriebsphase überprüft werden. Temporäre Zugangskonten, die nur während der Inbetriebnahme verwendet werden, sollten gelöscht werden.

Das Inbetriebnahme-Management bleibt auch während des Betriebs entscheidend. So kann beispielsweise der Neustart eines Systems die Berücksichtigung eines definierten Automatisierungsablaufs erfordern, weshalb klar sein sollte, welche Systeme zusammen und in welcher Reihenfolge neu gestartet werden müssen. Auch bei der Aktualisierung der Systeme ist Vorsicht geboten. Wiederinbetriebnahme-Pläne sind für eine wirksame Notfallplanung und den sicheren Betrieb der Anlage unerlässlich.

Während der Inbetriebnahme-Phase eines Gebäudeleitsystems können mehrere Techniker – darunter auch einige freiberufliche Auftragnehmer – auf technische Datenbanken zugreifen. Sicherheitsfunktionen wie Firewalls werden manchmal deaktiviert, um die Inbetriebnahme und Fehlersuche zu beschleunigen. Es ist wichtig, diese Handlungen zu dokumentieren und geeignete Maßnahmen zur Risikominderung zu ergreifen.

5.1.3. INF.14.A3 Sichere Anbindung von TGA-Anlagen und GA-Systemen

Technische Gebäudeausrüstung (TGA) bezeichnet alle im Bauwerk eingebauten oder damit fest verbundene technische Einrichtungen sowie technische Einrichtungen in Außenanlagen, die der funktionsgerechten Nutzung von Gebäuden dienen, wie zum Beispiel:

- Systeme für Gebäudeheizung und Trinkwassererwärmung
- Systeme zur Nutzung erneuerbarer Energien (Solarthermie, Geothermie, Photovoltaik, Biomasse)
- Stromversorgungsanlagen
- Informationstechnik, Melde- und Kommunikationsanlagen
- Feuerlöschanlagen oder Entrauchungsanlagen

Oft wird die Gebäudeautomation als ein Zusammenspiel verschiedener Gewerke-Teilsysteme betrachtet, anstatt als ein holistisches System. Darüber hinaus müssen häufig TGA-Anlagen mit eigener Steuerung in die Gebäudeautomation (GA) integriert werden. Es ist wichtig zu definieren, ob kommunizierende TGA-Anlagen oder Gewerke-Teilsysteme in anderen Teilsystemen oder der übergeordneten Gebäudeautomation eigenständige Aktionen auslösen können und dürfen. Darüber hinaus ist es entscheidend zu bestimmen, inwieweit diese Aktionen steuerbar oder eingrenzbar sind. Die Integration von TGA-Anlagen und Gewerkteilsystemen in übergeordnete Strukturen erfordert geeignete Sicherheitsmaßnahmen sowie eine sorgfältige Planung und Prüfung aller Prozesse und Funktionen. Alle Abläufe müssen getestet, dokumentiert, regelmäßig aktualisiert und bei Bedarf angepasst werden.

Ist eine vollständige Integration eines Gewerkteilsystems – beispielsweise Zugangskontrolle oder Notfall-Systeme – nicht möglich oder gewünscht, sollten Art und Umfang des Datenaustauschs mit der GA definiert werden.

Im Planungsprozess sind sämtliche relevanten Gewerksteilsysteme, Schnittstellen und kritische Parameter systematisch zu erfassen. Wo es geht, empfiehlt sich ein sequenzieller Anschluss an die GA, um Fehler schnell aufzuspüren und zu beheben.

Wichtige Schritte für die Integration:

- Jedes GA-Teilsystem (z. B. KNX) und seine Komponenten einzeln testen.
- Probleme im Einzelsystem vor der GA-Anbindung beheben.
- Autonome Betriebsfähigkeit der Teilsystem auch im Notfall sicherstellen.
- Schrittweise Integration einzelner Teilsysteme mit der GA testen.
- Nur definierte Daten und Aktionen zwischen der übergeordneten Gebäudeautomation und TGA oder Gewerke-spezifischen Teilsystemen erlauben.
- Kommunikation auf autorisierte Kanäle und Methoden beschränken.
- Probleme vor der nächsten Verbindung oder dem Vollbetrieb lösen.

Integration von Gebäudesystemen

Gewerkspezifische Steuerungssysteme, beispielweise eine KNX-Raumsteuerung, können mithilfe von Schnittstellen mit einer zentralen GA-Komponente (Visualisierung oder SCADA) oder mit anderen GA-Teilsystemen verbunden werden. Für eine erfolgreiche Integration ist eine präzise Planung sowie die Durchführung umfassender Tests unerlässlich.

Mindestanforderungen:

- Bei der Einrichtung sind die zulässigen Bereiche für alle wichtigen Parameter festzulegen, z. B. für die Höchst- und Mindestwerte oder die Heizungssollwerte.
- Es ist festzulegen, welche automatisierten Aktionen über eine Schnittstelle zu einem Gewerkseilsystem ausgelöst werden können, entweder durch Gebäudeautomation (GA) oder andere Gewerkseilsystemen

Die Teilsysteme werden häufig von unterschiedlichen Gewerken bereitgestellt. Daher ist es erforderlich, die Schnittstellen zwischen TGA- beziehungsweise GA-Systemen sorgfältig zu definieren. Zudem muss berücksichtigt werden, dass die Übergabe der Systeme in unterschiedlichen Projektphasen erfolgen kann. Verzögerungen und Abweichungen innerhalb eines Gewerkes können signifikante Auswirkungen auf andere Gewerke haben.

Mit der Einführung verschlüsselter Kommunikation in GA-Systemen sind im Bereich der Cybersecurity neue Herausforderungen entstanden. Oft stehen sicherheitsrelevante Informationen erst nach Inbetriebnahme zur Verfügung, was die Entwicklung von Schnittstellen verzögert; Systemänderungen im letzten Moment können darüber hinaus eine Aktualisierung der Sicherheitsdaten erfordern. Der Austausch eines KNX DATA Secure Geräts verändert z.B. die Sicherheitsschlüssel, die zur Entschlüsselung von KNX-Telegrammen in Überwachungs- oder Visualisierungssystemen nötig sind. Nach dem Gerätetausch müssen auch die Sicherheitseinstellungen angebundener Systeme aktualisiert werden.

KNX und BACnet legen ihre eigenen Sicherheits- und Kommunikationsstandards für Gateways fest, treffen jedoch keine Regelungen hinsichtlich der Sicherheit oder Funktionalität von Drittanbieter-Clients, die Daten über diese Gateways empfangen. Es ist daher empfehlenswert, entsprechende Sicherheitseigenschaften explizit in der Projektspezifikation zu berücksichtigen.

.

5.1.4. INF.14.A4 Berücksichtigung von Gefahrenmeldeanlagen in der GA

Sicherheits- und Schutzsysteme sind so mit Gebäudeautomationssystemen zu verbinden, dass Rückkopplungen ausgeschlossen werden und eine Trennung von der vollständigen GA-Integration gewährleistet ist. Für die Netzwerkanbindung empfiehlt sich der Einsatz physisch separierter Netzwerkelemente und -segmente. Die Verwendung zertifizierter und standardisierter Protokolle stellt sicher, dass Komponenten verschiedener Hersteller zuverlässig integriert werden können.

Die nachfolgenden Vorgaben betreffen die Einbindung von Sicherheits- und Schutzsystemen in Netzwerke:

- Kritische Systemsegmente sind so zu gestalten, dass sie sowohl funktionale als auch technische Unabhängigkeit aufweisen. Dadurch bleibt der Betrieb dieser Segmente auch im Falle von Konnektivitätsstörungen oder Datenverlusten innerhalb des übergeordneten Netzwerks sichergestellt.
- Zur Realisierung einer optimalen Systemperformance sollte eine konsequente physische Trennung, beispielsweise durch spezielle Verkabelung und Hardware, vorgesehen werden. Kritische Komponenten sind so auszugestalten, dass sie unabhängig von externen Netzdiensten betrieben werden können und ihre Funktionsfähigkeit auch bei Ausfällen anderer Netzwerksegmente oder Systeme erhalten bleibt.
- Netzwerkverbindungen zu weiteren Systemen sind strikt zu steuern, um etwaige Beeinträchtigungen des Alarmsystems – beispielsweise durch fehlerhafte oder unbefugte externe Signale und Daten – auszuschließen. Hierzu sind geeignete Sicherheitsmechanismen wie Firewalls einzusetzen, die Daten- und Signalflüsse gezielt kontrollieren und regulieren. Alternativ kann eine unidirektionale Übertragung implementiert werden, die ausschließlich einen abgehenden Informationsfluss ermöglicht.
- Jegliche nicht autorisierte oder unnötige Kommunikation mit kritischen Systemsegmenten ist zu unterbinden. Bei Auswahl von Funktechnologien und Frequenzbändern sind Maßnahmen vorzusehen, um Interferenzen zwischen verschiedenen Alarmanlagen sowie anderen Geräten zu vermeiden (siehe INF.14.M15 und INF.14.M16).

KNX-Systeme werden in der Regel nicht für sicherheitsbezogene Anwendungen eingesetzt. Bei geplanten sicherheitsrelevanten Anwendungen ist zu prüfen, ob eine Geräte- und Kommunikationsüberwachung oder ein definierter Notbetrieb erforderlich sind.

5.1.5. INF.14.A5 Dokumentation von Gebäudeautomation (GA)

Eine vollständige und aktuelle Dokumentation unterstützt das Systemmanagement. Regelmäßige Überprüfungen und Aktualisierungen stellen sicher, dass der Systemstatus korrekt wiedergegeben wird. Eine präzise Dokumentation erleichtert die Problemanalyse, die Identifizierung von Abhängigkeiten sowie die Bewertung von Änderungen.

Alle aktivierten und deaktivierten physischen Kommunikationsschnittstellen, Protokolle und Zugangspunkte der Gebäudeautomation (GA) sind zu dokumentieren. Zudem sind Wechselwirkungen und Abhängigkeiten zwischen GA-Komponenten und allen verbundenen technischen Systemen zu erfassen. Die Sicherheitsmerkmale der eingesetzten Protokolle sind in die Dokumentation aufzunehmen.

Änderungen sind zu dokumentieren. Es sollten systematische Überprüfungen erfolgen, um Änderungen oder Ausnahmen zu erkennen und entsprechend zu behandeln. Das Format der Dokumentation ist an die Anforderungen der jeweiligen GA-Installation anzupassen. Je nach Bedarf kann sie für einzelne Systeme getrennt oder konsolidiert geführt werden. Um die Kompatibilität sicherzustellen, sind Datenstruktur und erforderlicher Inhalt für jedes System

einschließlich angeschlossener Gewerkseilsysteme zu definieren. Eine zentrale Ablage, beispielsweise auf einer Online-Plattform, erleichtert Zugriffs- und Austauschmöglichkeiten.

Die Dokumentation muss jederzeit verfügbar sein, auch bei Ausfällen oder Notfällen. Dies kann durch Sicherungskopien auf Notfallsystemen oder bereitgestellte Druckversionen gewährleistet werden. Maßnahmen zum Schutz vor unbefugtem Zugriff sind zu berücksichtigen.

Bestandsdokumentationen sind oft aufwändig und werden meist vom Elektroinstallateur erstellt, da Systemintegratoren als Subunternehmer selten zuständig oder dafür ausgestattet sind. Die physische Installation ist in der Regel gut dokumentiert, während Angaben zu Sicherheit und Inbetriebnahme häufig fehlen.

5.1.6. INF.14.A6 Separierung von Netzen der GA

Das von der Gebäudeautomation genutzte OT-Netze sollten zumindest logisch von allgemeinen IT-Netzen und anderen institutionellen Netzen getrennt sein. Die Kommunikation zwischen Gebäudeautomation (GA) und anderen IT-Systemen ist zu überwachen und zu steuern. Um dies zu gewährleisten, sind Sicherheitsvorrichtungen wie Firewalls an allen Übergangspunkten zwischen diesen Netzen einzurichten.

In der Vergangenheit wurden für die Gebäudeautomation ein technisches Netzwerk eingerichtet und physisch vom Unternehmensnetzwerk isoliert. Heutzutage erfordert die Integration der Gebäudeautomation mit Gebäudemanagement- und Büro-IT-Systemen häufig eine zentrale Verwaltung über mehrere Standorte hinweg. Separate physische Netze für jede Gebäudeautomation werden daher meist nicht mehr umgesetzt.

Bei standortübergreifendem Einsatz können OT-Netze über Campus- oder dem Internet (VPN) verbunden werden, sollten jedoch durch Technologien wie VLANs logisch voneinander getrennt bleiben. Zugriffe von außen oder durch Dritte sind einer sorgfältigen Kontrolle zu unterziehen. Firewalls dienen dem Schutz der OT-Netze vor Zugriffen aus anderen Netzen und können idealerweise nach Anwendungen segmentiert werden. Eine räumliche Trennung ist nicht in jedem Fall erforderlich. Bei Fernwartungszugriffen durch Dritte sind geeignete Fernzugriffsprotokolle anzuwenden.

Internetzugang:

Teilen sich die Gebäudeautomation (GA) die Internetverbindung mit anderen Anwendung, muss diese sicher getrennt und GA-konform abgesichert werden. Bei separatem Netz gelten eigene Cybersecurity-Regeln; nur notwendige ausgehende Verbindungen sind erlaubt.

Trennung der Netzdienste:

Gebäudeautomation (GA) stellt Anforderungen an die Sicherheit und Verfügbarkeit von Netzdiensten. Diese müssen entsprechend den Standards ausgelegt sein.

IT-Möglichkeiten den Netzwerkzugang von GA-Komponenten zu kontrollieren

- Dedizierte, markierte VLAN-Ports auf gemeinsamen Switches
- Netzwerkzugriffskontrolle nach Ports
- Gegebenenfalls separate physische Switches für GA

Meist werden IT- und OT-Netzwerke über ein physisches Netz virtualisiert. Dabei entstehen Herausforderungen:

- OT-Netze müssen früh betriebsbereit sein, IT-Netze erst nach Gebäudeübergabe.
- IT-Systeme werden durch Mieter gestellt, OT-Netz-Aufgaben sind oft nicht festgelegt.
- IT-Abteilungen verlangen teils Sicherheitsfunktionen, die GA-Komponenten nicht bieten.
- Unterschiedliche Kenntnisse erschweren Abstimmung zwischen GA-Systemintegratoren und IT-Abteilungen.

Effektive Kommunikation zwischen IT und GA-Systemintegrator ist entscheidend.

5.2. Standard-Cybersecurity-Anforderungen (Sollte-Anforderungen)

Neben den grundlegenden Anforderungen werden die folgenden Kriterien als dem aktuellen Stand der Technik entsprechend betrachtet und sollten in der Regel eingehalten werden.

5.2.1. INF.14.A7 Festlegung einer Cybersecurity-Richtlinie für die Gebäudeautomation

Eine Sicherheitsrichtlinie für Gebäudeautomationssysteme legt in Übereinstimmung mit allgemeinen Sicherheits- und IT-Richtlinien die Anforderungen an Cybersecurity fest. Die Richtlinie stellt einen Rahmen zur Definition relevanter Vorgaben und Strategien im Bereich Gebäudeautomation dar. Sie ist keine technische Spezifikation oder ein spezielles Anforderungsdokument, sondern enthält allgemeine Prinzipien für sämtliche Systeme und Komponenten der Gebäudeautomation und -steuerung.

Diese Richtlinie einschließlich eventueller Aktualisierungen sollte allen Beteiligten im Bereich Gebäudeautomation zugänglich gemacht werden. Durch regelmäßige Information werden alle Parteien über die bestehenden Sicherheitsrichtlinien unterrichtet. Die Einhaltung der Richtlinie kann fortlaufend überprüft werden, etwa durch einen Abgleich mit geltenden Standards.

Wichtige Themen der Projektsicherheitsrichtlinie sind:

- Identifikation von TGA-/GA-Subsystemen mit GA-Schnittstellen.
- Kriterien für Systeme, die isoliert und ohne Rückwirkung betrieben werden sollen, mit klar abgegrenzter GA-Schnittstelle.
- Vorgaben für Auswahl und Nutzung von Tools wie ETS. Für KNX-Systeme sind Vorgaben zur Verwaltung von ETS-Passwörtern und Gerätezertifikaten zu dokumentieren.
- Maßnahmen zur sicheren Integration weniger cyberresilienter Komponenten und Anforderungen an neue Bauteile gemäß aktuellen Sicherheitsstandards.
- Richtlinien für Fernwartungstools mit Zugriff auf GA-Netze.
- Physische Sicherheit, Zugangsbeschränkungen und dokumentierte Authentifizierung; Systemzugriffe nur mit persönlichen Konten. Bei GA-Komponenten und Subsystemen ist eine geeignete Zuordnung der Nutzerrollen und Berechtigungen zu gewährleisten.
- Sicherheitsanforderungen und Protokolle für die Kommunikation sowie Regeln für Ausnahmen.
- Überwachungsrahmen und Festlegung der zu überwachenden Komponenten.

Abhängig von den jeweiligen institutionellen Rahmenbedingungen kann eine übergeordnete Sicherheitsrichtlinie sowohl das technische Gebäudemanagement als auch die Gebäudeautomation (GA) umfassen. Dabei sind jedoch stets die spezifischen Sicherheitsanforderungen der Gebäudeautomation (GA) zu berücksichtigen.

Wird das technische Gebäudemanagement durch einen externen Dienstleister erbracht, während die Gebäudeautomation (GA) weiterhin von der Institution selbst verwaltet wird, ist es erforderlich, die Sicherheitsrichtlinie für das technische Gebäudemanagement an die bestehende Sicherheitspolitik für die Gebäudeautomation (GA) anzupassen

5.2.2. INF.14.A8 Anforderungsspezifikation für GA-Systeme

Die Spezifikationen müssen sämtliche relevanten Aspekte im Hinblick auf Architektur, Design und Schnittstellen der einzelnen Systeme umfassend abdecken. Diese Dokumente sind fortlaufend an den aktuellen Stand der Technik anzupassen und während der Implementierungsphase regelmäßig zu prüfen.

Die Anforderungsspezifikation definiert die Sicherheitspolitik der Gebäudeautomation (GA) in einem zweistufigen Ablauf: Zunächst erfolgt eine detaillierte Analyse zur Erhebung und Strukturierung aller Anforderungen; darauf aufbauend werden spezifische Vorgaben für sämtliche einschlägigen GA-Komponenten festgelegt.

Gemäß der Cybersecurity-Richtlinie sollte die Spezifikation Folgendes vorsehen:

- Eine vollständige Anforderungsspezifikation für die Gebäudeautomation (GA).
- Separate Anforderungsspezifikationen für jedes Gebäudeautomation (GA)-Teilsystem, sollten TGA-Anlagen oder Geräte ein Kommunikationsschnittstelle haben ist auch diese zu berücksichtigen.
- Nachweis der Einhaltung der einschlägigen Rechts- und Verwaltungsvorschriften.

Detaillierte Anforderungsanalyse

In der Analysephase werden die organisatorischen und technischen Voraussetzungen für den Betrieb der Gebäudeautomation (GA) ermittelt. Dazu zählen die Planung von Anforderungen, Integrationsspezifikationen sowie das Einholen von Kundenfeedback. Funktionale und nicht-funktionale Anforderungen, insbesondere im Hinblick auf Informationssicherheit und Zugangspunkte der GA, werden bewertet.

Bei neuen Einrichtungen, bei denen die Nutzergruppen noch nicht definiert sind, empfiehlt es sich, zumindest allgemeine GA-Anforderungen bereits in der Planungsphase festzulegen, um spätere Anpassungen zu ermöglichen.

Ebenso sollten betriebliche Aspekte in die Analyse einbezogen werden. Der Betrieb der GA setzt in der Regel geschultes Personal voraus. Es kann vorkommen, dass aufgrund eingeschränkten Supports außerhalb der regulären Geschäftszeiten spezielle Anforderungen entstehen; zum Beispiel müssen Probleme mit wichtigen Komponenten der HLK-Anlage gegebenenfalls über Nacht durch vorkonfigurierte Ersatzgeräte behoben werden. Die Anforderungen an die betriebliche Sicherheit, einschließlich des Vorfallmanagements, sollten ebenfalls überprüft werden.

Anforderungsspezifikation

Das Spezifikationsdokument fasst die aus der Analyse abgeleiteten organisatorischen und technischen Anforderungen an die Informationssicherheit zusammen und bezieht sämtliche relevanten Komponenten der Gebäudeautomation sowie Betriebsparameter ein. Es enthält definierte Anforderungen an die Netzarchitektur und Infrastruktur. Maßnahmen zur Skalierbarkeit des Systems stellen sicher, dass gegenwärtige und zukünftige betriebliche Anforderungen berücksichtigt werden. Durch die systematische Priorisierung und Dokumentation aller Anforderungen kann während der Beschaffung auf die Spezifikationen verwiesen werden, wodurch das Risiko ungeeigneter Käufe reduziert wird.

Die Spezifikationen sollten mindestens folgende Anforderungen umfassen:

- Spezifikationen für IT-Systeme und deren Schnittstellen, beispielsweise Webbrowser mit Zugriff auf die Gebäudeautomation (GA)
- Definition zulässiger Zugriffsmethoden, wie etwa Fernzugriff
- Festlegung von Nutzerrollen und Berechtigungen
- Angabe der erlaubten Protokolle für den Zugang
- Identifizierung erforderlicher Sicherheitseigenschaften, einschließlich Verschlüsselung, Authentifizierung, Autorisierung sowie Integritätsprüfung
- Zugangsbeschränkungen, inklusive Notfallprotokollen
- Definition administrativer Sicherheitsverfahren, wie zum Beispiel das Vier-Augen-Prinzip bei administrativen Tätigkeiten

Das GA-Pflichtenheft bildet die zentrale Grundlage sowohl für die Konzeptentwicklung als auch für die anschließende detaillierte Arbeitsplanung.

5.2.3. INF.14.A9 Entwicklung eines GA-Konzepts

Ein umfassendes Konzept für die Gebäudeautomation (GA) ist unter Berücksichtigung der einschlägigen Richtlinien und Normen zur Cybersecurity zu entwickeln. Für das Gebäudeautomationssystem wird eine detaillierte Strategie benötigt, die sämtliche integrierten oder verbundenen Subsysteme, alle Komponenten der Gebäudeautomation sowie deren Kommunikationsverbindungen berücksichtigt.

Das Konzept hat sowohl technische als auch organisatorische Anforderungen, klar zu definieren und ist bei Bedarf regelmäßig zu überprüfen und anzupassen. Die GA sollte Abhängigkeiten zwischen Segmenten und Teilsystemen auf ein Minimum reduzieren, um potenzielle Störungen lokal eingrenzen zu können. Eine separate Steuerbarkeit jedes Gebäudesegments sowie die transparente Darstellung der eingerichteten Segmente sind sicherzustellen.

Das Konzept stellt eine wesentliche Grundlage für einen verlässlichen und wirtschaftlichen Betrieb dar, indem es Architektur, Aufgaben und Regelungen für den Routinebetrieb sowie für Systemänderungen eindeutig festlegt. Es dient als strukturgebender Rahmen, der bereits in der Planungsphase detailliert ausgearbeitet und hinsichtlich organisatorischer und technischer Aspekte ergänzt wird.

Das GA-Konzept umfasst unter anderem folgende Aspekte:

- Systemarchitektur und Segmentierung
- Beschreibung der Funktionen und Automatisierungsdiagramme
- Schnittstellen zu anderen Systemen

- Abhängigkeiten aufgrund von Systemvorgaben
- Kommunikationsprotokolle
- Netzwerksegmentierung
- Maßnahmen zur Sicherstellung der Verfügbarkeit (z. B. Redundanz)
- Rollenbasierte Berechtigungsstrukturen
- Zugangskontrollmechanismen

Eine regelmäßige Überprüfung und Anpassung des GA-Konzepts ist erforderlich, um die aktuellen technologischen Entwicklungen und bewährten Praktiken widerzuspiegeln. Hierdurch wird gewährleistet, dass das Konzept mit dem bestehenden System übereinstimmt und unerlaubte Änderungen rechtzeitig erkannt werden.

Aus unternehmerischer Sicht ist es wichtig, die vertraglichen und technischen Grenzen der jeweiligen Gewerksteilsysteme klar zu definieren und einzuhalten. Aufgaben sowie Hardware sollten eindeutig einem entsprechenden Vertrag zugeordnet werden.

Im Zuge der Umstellung auf verschlüsselte Kommunikation kann es notwendig sein, Zertifikate oder Kennwörter innerhalb eines Subsystems anzupassen, was Auswirkungen auf die Integration mit anderen Subsystemen haben könnte. Es empfiehlt sich, Schnittstellen frühzeitig zu identifizieren, an denen potenzielle Beeinträchtigungen auftreten könnten.

Das Steuerungskonzept sollte flexibel genug gestaltet sein, um sicherzustellen, dass bei sicherheitsrelevanten Anpassungen in Teilsystemen die Hauptfunktionen des Gebäudeleitsystems weiterhin zuverlässig ausgeführt werden. Kritische Kontrollfunktionen müssen selbst dann gewährleistet sein, wenn Sicherheitsdetails noch nicht vollständig aktualisiert wurden.

5.2.4. INF.14.A10 Bildung von unabhängigen GA-Bereichen

Die Segmente eines Gebäudeeinrichtungssystems werden idealerweise so gestaltet, dass sie möglichst geringe Abhängigkeiten voneinander aufweisen. Auf diese Weise kann jedes Segment eigenständig verwaltet werden, und Störungen in einem Bereich wirken sich kaum oder gar nicht auf andere Bereiche aus.

Standardisierung von Gebäudeautomation (GA)-Bereichen für mehr Effizienz und Stabilität

GA-Subsysteme mit ähnlichen Funktionen, wie z. B. Raumsteuerung, sollten idealerweise auf der gleichen Technologie basieren. Dies vereinfacht die Planung, unterstützt den täglichen Betrieb und trägt zur Systemstabilität bei. Befinden sich auf einer Etage mehrere Büros oder Besprechungsräume mit jeweils eigener Beleuchtungs-, Beschattungs- und Klimasteuerung, empfiehlt es sich, diese GA-Funktionen lokal zu verwalten. Nach Möglichkeit sollte ein GA-Segment oder eine Zone, die mehrere Bereiche umfasst, auch im Falle eines Ausfalls des Hauptsystems weiterhin betriebsbereit sein.

Netzarchitektur und Segmentierung

- Um den zuverlässigen Betrieb sicherzustellen, empfiehlt es sich, die Bereiche der Gebäudeautomation (GA) in Teilnetze zu unterteilen:
- Teilnetz-Isolierung: GA-Segmente oder -Bereiche sollten jeweils einem eigenen Subnetzzugeordnet werden. Dies reduziert das Risiko wechselseitiger Beeinträchtigungen, etwa durch Fehlermeldungen eines Geräts oder Probleme bei der Verkabelung.
- Sichtbarkeit des Managements: Jedes GA-Teilnetz sollte eindeutig identifizierbar und kontrollierbar sowie mit einem geeigneten Managementsystem oder Inbetriebnahme Werkzeugen wie ETS verwaltbar sein.

Sicherheit und Segmentierung

- **Dedizierte Netzwerkkomponenten:** Für jeden GA-Bereich ist die Ausstattung mit eigenen Netzwerkgeräten oder VLAN-Ports vorzusehen um die Sicherheit zu gewährleisten. Diese Geräte müssen über geeignete Filterfunktionen verfügen.
- **Planung von IP-Adressen**: Die IP-Kommunikation zwischen Gebäudeautomations-Bereichen sollte entsprechend den Sicherheitsanforderungen durch Firewalls gesteuert werden. Firewalls sind zu dokumentieren, da fehlende Dokumentation die Fehlersuche erschwert und verzögert.

Planung der Bereiche und deren Abhängigkeiten

- Vor der Festlegung von (GA)-Bereichen sind alle Abhängigkeiten zwischen Subsystemen und der Gebäudeautomation zu erfassen und zu dokumentieren.

Firewall und Zugangskontrolle

- **Kontrollierte Kommunikation**: Abhängig von den Sicherheitsanforderungen kann die Kommunikation mit Gebäudeautomationsbereichen durch Filterfunktionen reguliert werden.
- **Firewalls**: Firewalls bieten eine Option zur Trennung von Gebäudeautomationsbereichen, ohne dass Änderungen an der Subnetzstruktur erforderlich sind. Sie ermöglichen eine Steuerung innerhalb eines Teilnetzes.
- **Dokumentation**: Die Dokumentation von Firewalls ist erforderlich; fehlt diese, können Fehlerbehebungen erschwert und verzögert werden.

KNX-Systeme unterstützen diese Anforderungen, indem sie Linien, Bereiche und Segmente logisch und elektrisch trennen. Funktionen werden gezielt auf einzelne Segmente verteilt.

5.2.5. INF.14.A11 Absicherung von frei zugänglichen Ports und Zugängen der GA

Der Zugang zu IP-Netzwerken wird durch Einstellungen des OT-Netzwerks und durch Administratoren verwaltet. Der Zugriff auf Geräte, Dienste und Daten der Gebäudeautomation (GA) erfolgt gemäß den jeweiligen Einstellungen der Gebäudeautomation.

Die Verbindung nicht autorisierter oder unbekannter Geräte mit dem Gebäudeautomations- und Kontrollsystemnetzwerk ist zu kontrollieren und einzuschränken. Angeschlossene Geräte werden protokolliert, und unbefugte Kommunikation im OT-Netzwerk wird blockiert. Mithilfe der Netzwerkzugangskontrolle können nicht autorisierte Geräte isoliert werden. Temporäre nicht lokale Wartungsschnittstellen (VPN-Ports) werden ausschließlich bei Bedarf aktiviert.

5.2.6. INF.14.A12 Nutzung sicherer Übertragungsprotokolle für die GA

Für die Kommunikation über Ethernet und IP, insbesondere in nicht vertrauenswürdigen Netzwerken, sollten stets sichere Protokolle eingesetzt werden. Der IP-Verkehr im Bereich der Gebäudeautomation (GA) ist durch etablierte Verschlüsselungsstandards wie z.B. KNXnet/IP Secure, OPC-UA oder BACnet/SC zu schützen.

Sensible Daten, die außerhalb nativer und standardisierter GA-IP-Protokolle übertragen werden, sind über zeitgemäße sichere Kommunikationsprotokolle wie HTTPS (für Webinhalte) bzw. FTPS (für Dateiübertragungen), jeweils mit gültiger TLS-Verschlüsselung, abzusichern. Bei Verwendung proprietärer IP-Protokolle in Komponenten der Gebäudeautomation ist eine Sicherheitsbewertung vorzunehmen. Es ist sicherzustellen, dass diese Protokolle Verschlüsselungsmechanismen nutzen und nicht ausschließlich auf Intransparenz zur Absicherung setzen.

Ist eine IT-seitige Netzwerkzugangskontrolle nicht realisierbar, sind die Ports durch eine oder mehrere der folgenden Maßnahmen zu sichern:

- Einschränkung der Kommunikation am Zugangsschalter mittels Port Security,
- Konfiguration von Access Switch Ports an öffentlich zugänglichen GA-Komponenten zur Freigabe spezifischer IP-Adressen und Ports,
- Physische Sicherung der Ports, z. B. mit verschlossenen Schränken oder Portschlössern, um nur autorisierte Zugriffe zu ermöglichen.

5.2.7. INF.14.A13 Netzsegmentierung in der GA

Die Segmentierung eines Netzwerks ist ein wichtiger Aspekt. Dafür ist es erforderlich, Übergangsregeln zwischen den einzelnen Segmenten eindeutig festzulegen und mit Sicherheitskomponenten wie Routern oder Gateways abzustimmen. Eine Kommunikationsmatrix bildet die Grundlage und enthält Angaben zu den beteiligten Komponenten, externen Schnittstellen, verwendeten Protokollen und verantwortlichen Organisationen.

Innerhalb einzelner Segmente besteht in der Regel keine Einschränkung der Kommunikation. Die Verbindung zwischen verschiedenen Segmenten hingegen sollte geregelt und auf das notwendige Maß für den Betrieb begrenzt werden. Häufig werden Verbindungen von einem Segment mit höheren Sicherheitsanforderungen zu einem Segment mit niedrigeren Anforderungen eingerichtet. Firewalls dienen zur Steuerung und Überwachung der Kommunikation zwischen den Segmenten. Berücksichtigen Sie bei der Überprüfung der Segmentierung mindestens diese Bereiche:

- Komplette Gebäudeautomation (GA)
- Subsysteme des Gebäudeautomationssystems, z. B. KNX-, Modbus- oder BACnet-System.
- Individuelle Steuerung von Gewerkseilsystemen innerhalb eines Gebäudeautomation (GA)-Systems, z.B. der primären Anlagensteuerung
- Gebäudeautomation (GA)-Komponenten, die zu verschiedenen Benutzerorganisationen gehören, z. B. ein Gebäudeautomation (GA) Supervisor, der mit mehreren Gewerkseilsystemen und Protokollen verbunden ist

- Von verschiedenen Organisationen verwaltete Netzwerkbereiche

Die Netzwerksegmentierung innerhalb von Subnetzen ist gemäß relevanter Industriestandards wie z.B. KNX oder BACnet durchzuführen. Bei der Planung und Implementierung sind sowohl technische als auch nutzerspezifische Anforderungen sowie Abhängigkeiten zu berücksichtigen; dabei muss die Systemstabilität jederzeit gewährleistet bleiben. Bestehende Netzsegmente und die Kommunikationsmatrix sind regelmäßig zu überprüfen, insbesondere nach Änderungen wie System-Upgrades. Sämtliche Überprüfungen sind lückenlos zu dokumentieren, einschließlich aller sicherheitsrelevanten Komponenten wie Firewalls.

Mikro-Segmentierung von unsicheren Gebäudeautomation (GA)-Komponenten

Zur Absicherung der Gebäudeautomation empfiehlt es sich, weniger vertrauenswürdige Systemkomponenten zu isolieren, indem Geräte mit unverschlüsselter Kommunikation separiert und eine risikoorientierte Mikrosegmentierung implementiert werden. Für die Übertragung von Daten zwischen einzelnen Segmenten sollten verschlüsselte Proxys eingesetzt oder eine angemessene Transportverschlüsselung angewendet werden. Sowohl das KNX- als auch das BACnet-Protokoll stellen hierfür geeignete Mechanismen zur Verfügung. Die Verbindung der Mikrosegmente hat auf Basis definierter Sicherheitsrichtlinien zu erfolgen.

5.2.8. INF.14.A14 Nutzung eines GA-geeigneten Zugriffschutzes

Ein Identitäts- und Zugangsmanagementsystem für zentrale Gebäudeautomationsgeräte sollte spezifisch auf die Anforderungen der Gebäudeautomation (GA) abgestimmt sein. Dies kann entweder durch eine darauf ausgelegte GA-Authentifizierungslösung oder durch eine Integration mit dem zentralen IT-Authentifizierungssystem erfolgen.

Rollen und Berechtigungen sind klar zu definieren, etwa für Bediener des GA-Systems, technische Anlagenbetreiber und andere relevante Nutzer, besonders in komplexen, mehrstufigen Kontrollumgebungen. Es empfiehlt sich, Rollen wie Mieter und Betreiber eindeutig zuzuteilen und Berechtigungen auf die erforderlichen Funktionen zu begrenzen; zum Beispiel sollten Mieter lediglich Zugriff auf ihnen zugewiesene Bereiche erhalten. Nach organisatorischen Veränderungen, beispielsweise Mieterwechsel oder Bauarbeiten, müssen die Rollen zeitnah aktualisiert werden.

Die gängigen Berechtigungsstufen umfassen im Allgemeinen Nur-Lesen sowie Lesen/Schreiben. Volle Administrationsrechte sollten ausschließlich qualifiziertem Personal vorbehalten sein, insbesondere bei Neueinrichtung oder wesentlichen Änderungen.

Werkzeuge zur Inbetriebnahme und Projektdaten sind durch starke Passwörter abzusichern, und alle Zugriffe auf Engineering-Tools und Datenbanken sind zu protokollieren und zu überwachen.

IP-Geräte ohne Datenverschlüsselung, Portsicherheit oder Passwortschutz sollten möglichst ersetzt werden. Wartungsgeräte sind vom Hauptnetzwerk durch Segmentierung und Zugangskontrollen zu isolieren. Komponenten mit herstellerdefinierten Zugangsdaten, die nicht veränderbar sind, sollten vermieden werden.

Nach den EU-Vorschriften zur Cybersecurity-Resilienz müssen Hardware-Anbieter kostenlose Sicherheitsupdates für die durchschnittliche Lebensdauer des Produkts (mindestens fünf Jahre) bereitstellen; dies gilt jedoch ausschließlich für Sicherheitsupdates. Für diesen Zweck werden häufig Inbetriebnahme-Tools benötigt, um nach einem Update die korrekte Funktion der Anlage zu überprüfen. Es sollte überprüft werden, ob Software und Inbetriebnahme-Tools jederzeit verfügbar oder beziehbar sind und ob der Zugang von Wartungsverträgen oder Abonnements abhängt.

5.2.9. INF.14.A15 Absicherung von GA-spezifischen Netzen

Es empfiehlt sich, Gebäudeautomations-IP-Protokolle wie KNXnet/IP Secure, OPC UA oder BACnet/SC zu nutzen. Authentifizierung und Verschlüsselung werden empfohlen. Die Kommunikation mit spezifischen Netzen der Gebäudeautomation sollte überwacht und durch sicherheitsfähige Gateway-Komponenten eingeschränkt werden. Für diese Netze sollten Sicherheitsmaßnahmen angewandt werden, die mit den allgemeinen Sicherheitsrichtlinien der jeweiligen Organisation übereinstimmen.

Bei der Verschlüsselung der Kommunikation sollten aktuelle Industriestandards Anwendung finden. Beispielsweise nutzt BACnet/SC das TLS 1.3-Protokoll für IPv4 und IPv6, während KNX IP Secure die AES-128-Verschlüsselung einsetzt.

Sollte eine Gebäudeautomationskomponente nicht den erforderlichen Sicherheitsanforderungen genügen, ist zunächst eine umfassende Risikoanalyse durchzuführen. Insbesondere ältere Systeme entsprechen häufig aufgrund technischer Limitationen nicht aktuellen Sicherheitsstandards. Sofern diese Systeme nach erfolgter Risikobewertung weiterhin betrieben werden, ist ein strukturierter Stufenplan für deren zeitnahen Ersatz zu entwickeln. Bis zur vollständigen Ablösung sollten betroffene Komponenten in segregierten Teilnetzen betrieben und der Datenverkehr an den Netzanschlusspunkten konsequent überwacht sowie kontrolliert werden. Die Umsetzung kann beispielsweise durch den Einsatz von Gateways mit spezifischen GA-Sicherheitsmechanismen, wie etwa Sicherheits-Proxys, erfolgen.

Gateways zu GA-spezifischen Netzen müssen so konfiguriert werden, dass nur autorisierte Kommunikation möglich ist. Für Ethernet-basierte Gebäudeautomation GA-Netzwerke, wie z.B. BACnet/IP und KNXnet/IP, wird empfohlen, Switches einzusetzen, die Access Control Lists unterstützen.

Die Netzarchitektur sollte gewährleisten, dass es keine unbeabsichtigten Verbindungen oder Abkürzungen zwischen Netzsegmenten über Gebäudeautomation (GA)-Netze oder Gateway-Geräte gibt.

5.2.10. INF.14.A16 Absicherung von drahtloser Kommunikation in GA-Netzen

Gebäudeautomationssysteme verwenden unterschiedliche drahtlose Kommunikationsmethoden, darunter Wi-Fi, Bluetooth, Zigbee, LoRaWAN, EnOcean und KNX-RF. Diese Technologien sind jeweils mit eigenen Sicherheitsmerkmalen ausgestattet und nutzen häufig Verschlüsselungsstandards wie AES-128 oder AES-256 zum Schutz der übertragenen Daten.

Um drahtlose Gebäudeautomationsnetzwerke sicher zu betreiben:

- Für die drahtlose Kommunikation empfiehlt sich der Einsatz aktueller Verschlüsselungs- und Authentifizierungsverfahren nach dem jeweiligen Stand der Technik. Geräte oder Systeme, die keine sichere Kommunikation unterstützen, sollten geprüft und das Risiko bewertet werden. Der Ersatz unsicherer Geräte ist möglichst zeitnah zu planen.
- Es sollten ausschließlich bekannte und autorisierte Geräte mit dem drahtlosen Netzwerk verbunden sein.
- Drahtlose Störungen durch andere Geräte und Netzwerke, insbesondere im 2,4-GHz-Band (Wi-Fi, Zigbee usw.), sind zu prüfen. Eine sorgfältige Planung und Überprüfung kann Unterbrechungen vorbeugen.
- Die Priorisierung von Systemen bei Nutzung bestimmter Frequenzbänder dient dazu, eine Beeinträchtigung von Gebäudeautomationsgeräten zu vermeiden.
- Bei anhaltenden Störungen, die sich nicht durch Anpassungen beheben lassen, kann ein Wechsel zu einer anderen Funktechnologie oder Frequenz sinnvoll sein.
- Physikalische Hindernisse wie Stahlwände oder spezielle Fenster können die drahtlose Kommunikation einschränken. Das Gebäudelayout und die Funkabdeckung sollten vor der Implementierung überprüft werden.
- Der Einsatz drahtloser Kommunikation sollte in Bereichen mit starken Störungen, im Freien oder bei nicht lösbaren Frequenzkonflikten vermieden werden.

Diese Hinweise erhöhen die Sicherheit und Zuverlässigkeit drahtloser Gebäudenetzwerke und helfen, Störungen zu vermeiden.

5.2.11. INF.14.A17 Absicherung von Mobilfunkkommunikation in GA-Netzen

Bei der Einbindung von Mobilfunknetzen in Gebäudeautomations- und -steuerungssysteme ist es essenziell, sämtliche verfügbaren Sicherheitsmechanismen umfassend zu nutzen. Eine unkontrollierte IP-basierte Direktkommunikation mit GA-Komponenten über öffentliche Mobilfunknetze wie 5G oder Sigfox ist grundsätzlich zu vermeiden.

Low-Power Wide Area Networks (LPWAN), ursprünglich für IoT-Anwendungen entwickelt, finden teilweise Anwendung in der Gebäudeautomation. Sie ermöglichen energieeffizienten Geräten wie batteriebetriebenen Sensoren die Übertragung von Daten über große Distanzen zu einem definierten Gateway.

Der Anschluss von Komponenten der Gebäudeautomation an öffentliche Mobilfunknetze sollte ausschließlich auf Basis zwingender betrieblicher Notwendigkeit und nach einer sorgfältigen Bedarfsprüfung erfolgen. Fehlt eine geeignete Netzsegmentierung im öffentlichen Mobilfunknetz, empfiehlt sich der Einsatz eines Application Layer Gateways zur Isolation der IP-Kommunikation. Zudem wird die Verwendung von Kopplungselementen mit integrierten Firewall-Funktionen dringend angeraten, um mobile Netzwerke, die mit den Automations- und Steuerungssystemen verbunden sind, effektiv abzusichern.

Da die sicherheitstechnischen Eigenschaften je nach eingesetzter Mobilfunktechnologie variieren, ist vor Auswahl einer bestimmten Technologie zu überprüfen, inwieweit diese den spezifischen Sicherheitsanforderungen genügt. Bei Anbindungen an öffentliche Netze sollten Unternehmen die vom Anbieter bereitgestellten Sicherheitsmaßnahmen, insbesondere Verschlüsselung, evaluieren und gegebenenfalls weitere Verschlüsselungsmaßnahmen implementieren, um sensible Daten bestmöglich zu schützen. Geräte der Gebäudeautomation nutzen eventuell integrierte SIM-Karten für Verbindungen zu Cloud-Diensten oder externen Serviceprovidern; entsprechende Zugriffe sind durch Firewalls abzusichern, sodass ausschließlich temporärer, vom Endgerät initiierter Zugriff gestattet wird.

5.2.12. INF.14.A18 Sichere Anbindung von GA-externen Systemen

Die Kommunikation zwischen der Gebäudeautomation (GA) und externen Systemen hat ausschließlich über eindeutig definierte Schnittstellen mit spezifischen Cybersecurity-Merkmalen zu erfolgen. Eine Authentifizierung und

Verschlüsselung der Kommunikationswege ist zwingend erforderlich. Die Anzahl der Schnittstellen zu externen Systemen ist auf das erforderliche Minimum zu reduzieren.

Bei einer Verbindung der Gebäudeautomation (GA) mit externen Systemen, wie z. B. Büro-IT oder anderen Netzwerken, sind folgende Aspekte zu berücksichtigen:

- Sämtliche Verbindungen und Abhängigkeiten zwischen der GA und externen Systemen müssen dokumentiert werden.
- Die Kommunikation ist auf festgelegte Schnittstellen, Protokolle und Systeme zu beschränken und entsprechend zu kontrollieren.
- Externe Kommunikation ist grundsätzlich zu vermeiden und nur in begründeten Ausnahmefällen zuzulassen.
- Bei gemeinsamer Nutzung von Ressourcen (wie Netzwerken oder Verzeichnisdiensten) durch die GA und andere Systeme sind klare Regelungen hinsichtlich Verfügbarkeit, Informationssicherheit und Zugriffsrechten zu definieren.
- Verantwortlichkeiten für Änderungen und Wartungsarbeiten an gemeinsam genutzten Ressourcen müssen eindeutig festgelegt werden.
- Alle externen Parteien, die an der Nutzung gemeinsamer Ressourcen beteiligt sind, sind in die entsprechenden Vereinbarungen einzubeziehen.

5.2.13. INF.14.A19 Nutzung dedizierter Adressbereiche für GA-Netze

Dedizierte IP-Adressbereiche sind speziell für die Gebäudeautomation (GA) zuzuweisen und strikt von Bereichen der Büro-IT oder anderer Betriebstechnologiesysteme (OT) zu trennen. Es ist essenziell, klar zu definieren, welche Segmente des Adressraums für statische IP-Zuweisungen vorgesehen sind und für welche GA-Komponenten diese benötigt werden.

Die Vergabe von IP-Adressen sollte nach einem nachvollziehbaren, logischen System erfolgen, das sowohl das jeweilige Gebäude als auch den Gerätetyp eindeutig abbildet. Bei Einsatz von DHCP zur automatischen Adressvergabe ist auf eine konsequente Trennung zwischen dynamischen und statischen Adressbereichen zu achten. Da der überwiegende Teil der GA-Geräte mit statischen Adressen betrieben wird, ist ein durchdachtes Adresskonzept unerlässlich, um Konflikte zu vermeiden.

Werden Netzwerksegmente über mehrere Liegenschaften hinweg gespiegelt, sind Methoden wie Network Address Translation (NAT) einzusetzen, um Adresskonflikte auszuschließen. Es ist zudem zu berücksichtigen, dass gebäudetechnikspezifische Protokolle wie BACnet und KNXnet/IP nicht zwangsläufig von allen Netzwerktechnologien unterstützt werden. Zertifizierte KNXnet/IP-Router und Schnittstellen unterstützen die Einbindung via DHCP. Allerdings kann die umfassende Nutzung von DHCP bei KNXnet/IP-Clients, beispielsweise in Visualisierungssystemen, systembedingt eingeschränkt sein.

5.2.14. INF.14.A20 Vermeidung von Broadcast-Kommunikation in GA-Netzen

In OT-Netzwerken für die Gebäudeautomation ist der Broadcast-Verkehr auf den OSI-Schichten 2 (Datenverbindung) und 3 (Netzwerk) zu minimieren, um eine Überlastung zu vermeiden; verwenden Sie vorzugsweise Unicast oder Multi-cast, wann immer dies möglich ist. Verwenden Sie Broadcasts nur, wenn es unumgänglich ist, und segmentieren Sie das Netz richtig.

Konfigurieren Sie die Router der Gebäudeautomation (GA) so, dass Broadcasts nicht weitergeleitet werden, es sei denn, dies ist für bestimmte Subnetze erforderlich. Geräte mit Bedarf an Broadcast-Kommunikation sollten in einem gemeinsamen Subnetz zusammengefasst und von anderen netzwerktechnisch getrennt werden, um unerwünschte Reaktionen auf Broadcast-Verkehr zu vermeiden.

5.2.15. INF.14.A21 Anzeigen der Gültigkeit von Informationen in GA-Systemen

Bei fernüberwachten Gebäudeleitsystemen ist es notwendig, die Aktualität der angezeigten Daten – wie Werte oder Statusinformationen – eindeutig festzustellen. Das System muss erkennen, wenn kritische Daten veraltet sind und sollte entweder Nutzer informieren oder eine Fehlerreaktion auslösen, um den Schutz von Bewohnern und Gebäuden zu gewährleisten. Simulierte oder „eingefrorene“ Daten werden bei Bedarf gekennzeichnet oder lösen einen Alarm aus.

Viele KNX-Geräte senden regelmäßig Schlüsselwerte wie Temperaturen und Ventilstellungen und unterstützen Funktionen zur Kommunikationsüberwachung; wenn innerhalb eines bestimmten Zeitraums keine neuen Daten eintreffen,

wechseln sie in eine festgelegte Fehlerposition, wodurch der Schutz von Bewohnern und Gebäuden gewährleistet bleibt.

Diese Funktionen können in Überwachungssystemen genutzt werden, die beispielsweise die regelmäßige Übermittlung von Schlüsselwerten überprüfen oder Fehlermeldungen von KNX-Geräten im Rahmen der Kommunikationsüberwachung erfassen. Twisted-Pair-Geräte der Feldebene im KNX-System bieten keinen eigenen Anwender-Fehlermeldedienst, stellen aber Dienste zur Verfügung, die externe Überwachung ermöglichen.

5.2.16. INF.14.A22 Sicherstellung von autark funktionierenden GA-Systemen und TGA-Anlagen

Jedes Gebäudeautomationssystem und seine Segmente sollten unabhängig nach ihren Schutzanforderungen arbeiten und auch bei Ausfall der Verbindung zur zentralen Gebäudeautomation (GA) betriebsbereit bleiben. Kritische Abhängigkeiten zu zentralen Komponenten oder anderen Segmenten sind zu minimieren. Die Systeme müssen für eine dem Schutzniveau entsprechende Zeit eigenständig funktionieren.

Abhängigkeiten zwischen Gewerkseilsystemen, Geräten und angebundenen Systemen sind zu identifizieren; die Mindestbetriebsdauer pro System muss definiert sein. Geräte, die kontinuierlichen Internetzugang benötigen, sollten durch Alternativen ersetzt oder mit einer sicheren, dedizierten Verbindung ausgestattet werden. Segmentierung ist ein grundlegendes Prinzip für jedes gute KNX-Systemdesign.

5.2.17. INF.14.A23 Einsatz von physisch robusten Komponenten für die GA

Je nach Betriebsbedingungen ist der Einsatz langlebiger Komponenten in der Gebäudeautomation (GA) besonders unter anspruchsvollen Umgebungsbedingungen zu empfehlen. Stehen solche robusten Bauteile nicht zur Verfügung, sind geeignete Kompensationsmaßnahmen zu treffen. Der KNX-Standard schreibt zudem vor, dass zertifizierte KNX-Produkte über eine Mindestbetriebsdauer von zehn Jahren verfügen müssen.

5.2.18. INF.14.A24 Zeitsynchronisation für die GA

Die zeitliche Synchronisation aller angeschlossenen Komponenten und Systeme ist sicherzustellen, sofern sie für automatisierte Mess-, Steuer- oder Regelungsprozesse erforderlich ist. Ebenso sollten sämtliche Einheiten der Gebäude-Automation (GA) auf eine einheitliche Zeitbasis zurückgreifen. Umfasst ein GA-System mehrere Gebäude oder Standorte, ist die Zeitsynchronisation über alle beteiligten Liegenschaften hinweg zu gewährleisten.

Bei Erfordernis einer Echtzeitkommunikation innerhalb des GA-Systems ist zur Zeitsynchronisierung vorzugsweise auf native Punkt-zu-Punkt-, Multicast- oder vergleichbare Verfahren – beispielsweise native KNX-Kommunikation – zurückzugreifen, anstatt ausschließlich auf das Network Time Protocol (NTP) zu setzen.

5.2.19. INF.14.A25 Dediziertes Monitoring in der GA

Für sicherheitskritische Komponenten der Gebäudeautomation ist es erforderlich, sicherheitsrelevante Laufzeitereignisse sowie die Verfügbarkeit der Geräte zu protokollieren. Ein umfassender Überwachungsplan sollte konzipiert und implementiert werden. Die Verfügbarkeit und wesentliche Parameter bauteilbezogener Systeme sind kontinuierlich zu überwachen. Bei Fehlern oder beim Erreichen definierter Grenzwerte muss eine automatische Benachrichtigung der Betriebsorganisation erfolgen. Die Gebäudeautomation muss mindestens Alarmmeldungen auslösen, wenn Systeme ausfallen oder zentrale Kontrollfunktionen nicht mehr verfügbar sind. Darüber hinaus ist festzulegen, welche sicherheitsrelevanten oder weiteren Ereignisse automatisch Alarme generieren sollen. Statusinformationen und Überwachungsdaten dürfen ausschließlich über geschützte Kommunikationskanäle übertragen werden.

Diese Anforderungen werden in der Regel auf Automatisierungs- oder Managementebene umgesetzt, wobei KNX die Überwachung bestimmter Ereignisse auf Feldebene ermöglicht.

5.2.20. INF.14.A26 Protokollierung in der GA

Neben der Anforderung, Statusänderungen zu protokollieren, ist auch die Erfassung sicherheitsrelevanter Ereignisse erforderlich. Sämtliche Konfigurationsänderungen an der technischen Gebäudeausrüstung, einschließlich Software- oder Firmware-Updates, sind lückenlos zu dokumentieren. Es ist festzulegen, welche Protokolldaten in einem zentralen Protokollierungssystem aggregiert werden. Da Änderungen beispielsweise die Verdrahtung, physische Modifikationen oder Konfigurationsanpassungen unter Einsatz externer protollspezifischer Tools umfassen können, ist es nicht immer möglich, valide Logdaten direkt vom Gebäudeautomationssystem (GA) zu beziehen. In solchen Fällen wird auf Inbetriebnahme- und Standortberichte zurückgegriffen, die von Installateuren, Wartungspersonal oder Systemintegratoren erstellt werden. Die Übertragung von Protokolldaten hat grundsätzlich über gesicherte Kommunikationskanäle zu erfolgen.

Bei KNX-Systemen werden Konfigurationsänderungen über die ETS vorgenommen; Änderungen werden dabei erfasst.

5.2.21. INF.14.A27 Berücksichtigung von Wechselwirkungen zwischen Komponenten der GA in der Notfallplanung

Eine regelmäßige Bewertung der Auswirkungen von Gebäudeautomation (GA) auf die Notfallplanung ist erforderlich. Es sollten Richtlinien zur Minimierung von Störungen entwickelt werden, falls GA-Komponenten aufgrund technischer Probleme oder Cyberangriffen ausfallen. Notfallpläne müssen Kontaktinformationen für das Instandhaltungspersonal sowie die zuständigen Ebenen für die Bewältigung von Notfällen beinhalten.

Verfahren zur Aufrechterhaltung wesentlicher Betriebsabläufe bei Ausfall der Gebäudeautomation (GA) sind zu skizzieren. Wiederanlaufpläne für alle Systeme sollten dokumentiert werden, einschließlich der Reihenfolge des Wiederanlaufs.

Notfall- und Fehlerbehebungsverfahren sind auch für Zeiträume zu berücksichtigen, die über Mängel und Wartungsverträge hinausgehen, da die Gebäudeleitsysteme eine Lebensdauer von mehr als zehn Jahren haben können. In diesem Zeitraum besteht die Möglichkeit, dass Lieferanten ihre Tätigkeit einstellen oder Verträge auslaufen. Für KNX-Anlagen wird ein langfristiger Support bereitgestellt, sofern ein gültiges ETS-Projekt und Projektpasswörter vorhanden sind.

5.3. Anforderungen für kritische Systeme mit erhöhten Anforderungen an die Cybersecurity

Diese zusätzlichen Anforderungen erhöhen das Sicherheitsniveau. Sie sollten sie berücksichtigen, wenn die Risikobewertung einen erhöhten Schutz nahelegt.

KNX-Systeme sind üblicherweise nicht für Anwendungen vorgesehen, die besondere Sicherheitsanforderungen erfüllen müssen.

5.3.1. INF.14.A28 Physische Trennung der GA

Für einen optimalen Schutz empfiehlt es sich, Gebäudeautomationssysteme mit erhöhten Anforderungen an die Cybersecurity physisch zu isolieren. Sofern eine Verbindung zu externen Cloud-Diensten erforderlich ist, sollte diese ausschließlich über einen dedizierten und streng überwachten Internetzugang erfolgen. Darüber hinaus sind Verbindungen zu nicht vertrauenswürdigen Netzwerken, einschließlich des internen Büronetzes, gemäß den spezifischen Schutzanforderungen der Gebäudeautomation (GA) konsequent zu unterbinden.

5.3.2. INF.14.A29 Trennung einzelner TGA-Anlagen

Für Gebäudesysteme mit erhöhten Sicherheitsanforderungen, beispielsweise im Bereich Sicherheitssysteme, kann die Einrichtung eines separaten OT-Netzwerksegments zur Isolierung in Erwägung gezogen werden. Dies unterstützt die Überwachung und Steuerung der entsprechenden Kommunikation.

5.3.3. INF.14.A30 Bereitstellung eines GA-eigenen Zeitservers

Für eine erhöhte Systemsicherheit empfiehlt es sich, einen dedizierten Zeitserver für die Gebäudeautomation (GA) oder für spezifische Gebäudeteilsysteme zu implementieren. Dieser Server sollte nicht nur das Network Time Protocol (NTP), sondern auch GPS oder eine alternative zuverlässige Zeitquelle integrieren.

6. Schlussfolgerung:

Ein störungsresistentes Gebäudeautomation (GA)-System ist auch gegen Cybersecurity-Risiken gut gewappnet.

Eine effektive Methode zum Schutz vor Cybersecurity-Bedrohungen ist ein strukturiertes und fehlertolerantes Gebäudeleitsystem. Bei ausreichender Segmentierung existieren keine zentralen Fehlerpunkte, da die Kontrollfunktionen verteilt und möglichst lokalisiert sind. Dieser Aufbau reduziert potenzielle Schwachstellen und trägt zur Sicherheit von Automatisierungslösungen wie KNX-Systemen bei. Eine konsequente Segmentierung und lokale Steuerung können das Risiko von Cyberangriffen senken.