CYBERSECURITY IN DER GEBÄUDESTEUERUNGEN

Übersicht der Cybersecurity Planungshinweise für die Gebäudeautomation

Inhalt

1. Zweck des Dokuments **1**

2. Cybersicherheit für Gebäudeautomations- und -steuerungssysteme **2**

3. Schwachstellen des Gebäudeautomationssystems als Risikofaktoren **2**

4. Cybersecurity im Planungs- und Ausschreibungsprozess **2**

5. Cybersecurity von OT-Netzwerken **3**

6. Cybersecurity-Anforderungen Planen **3**

6.1. Bewertung des aktuellen Zustands 4

6.2. Verantwortlichkeiten und Rechenschaftspflicht für Cybersecurity 4

7. Cybersecurity-Anforderungen an die Gebäudeautomation (GA) **5**

7.1. Grundlegende Cybersecurity Anforderungen (Muss-Anforderungen) 5

7.2. Standard-Cybersecurity-Anforderungen (Sollte-Anforderungen) 6

7.3. Anforderungen für kritische Systeme mit erhöhten Anforderungen an die Cybersicherheit 9

Ein störungsresistentes GA-System ist auch gegen Cybersecurity-Risiken gut gewappnet. **9**

8. 9

1. Zweck des Dokuments

Dieser Überblick behandelt die Rolle der Cybersicherheit bei der Planung, Implementierung und dem Betrieb von Gebäudeeinrichtungen (GA). Dabei werden die Sicherheitsanforderungen auf Grundlage des IT-Grundschutz-Kompendiums des Bundesamtes für Sicherheit in der Informationstechnik (BSI) dargestellt.

2. Cybersecurity für Gebäudeautomations- und -steuerungssysteme

Die Gebäudeautomation steigert die Gebäudeeffizienz durch die Automatisierung von Funktionen wie Heizung, Lüftung, Beleuchtung und Sicherheit. IT-Sicherheit für das Gebäudemanagement ist aufgrund der sich ständig ändernden Vorschriften, Risiken und Möglichkeiten von entscheidender Bedeutung. Bedrohungen können intern sein und die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit des Systems beeinträchtigen, oder extern, wie Sabotage, Spionage oder unbefugter Zugriff.

3. Schwachstellen des Gebäudeautomationssystems als Risikofaktoren

Mehrere Faktoren können die IT-Sicherheit beeinträchtigen:

- Fehlende Berücksichtigung grundlegender IT-Sicherheitsaspekte bei der Planung
- Unzureichende Dokumentation mit lückenhaften oder fehlenden Aufzeichnungen
- Verwundbare Schnittstellen zwischen unterschiedlichen Systemen
- Mangelnde Überwachung, wodurch kritische Systemausfälle unerkannt bleiben können
- Schwächen im Rollen- und Zugriffsmanagement
- Lange Lebenszyklen von Gebäudesystemen

4. Cybersecurity im Planungs- und Ausschreibungsprozess

Häufig können Mieter und Nutzer während der Bauphase noch nicht identifiziert werden, was zu unklaren Cybersecurity-Anforderungen führt. Nach dem Einzug der Mieter sind unter Umständen Anpassungen der Systeme erforderlich. Zukünftige Nachrüstungen und Änderungen können kosten- und zeitintensiv sein, besonders wenn eine detaillierte Bestandsdokumentation fehlt.

Definierte Anforderungen
Das technische Gebäudemanagement erfolgt oft in verschiedenen Gewerken, was Verzögerungen und zusätzliche Kosten bei der Fehlerbehebung verursachen kann. Potenzielle Cybersecurity-Risiken an Gateways und Übergabepunkten werden mitunter nicht ausreichend berücksichtigt.

Ausreichende Dokumentation
Eine umfassende Dokumentation unterstützt die Umsetzung von Systemänderungen und hilft dabei, unnötige Ausgaben zu vermeiden.

Überwachung der Gebäudeautomation
Die Überwachung dient der Erkennung technischer Fehler und Sicherheitsvorfälle. Eine frühzeitige Festlegung geeigneter Überwachungsmethoden trägt zu einem effizienten Betrieb und zur Kontrolle des Systemzugangs bei.

Rollen- und Berechtigungsmanagement
Ein System zur Verwaltung von Benutzeridentitäten und Zugangsrechten unterstützt die Organisation der Zugriffsverwaltung. Die Überwachung und Verwaltung der Zugriffsrechte sollten möglichst früh im Prozess erfolgen.

5. Cybersecurity von OT-Netzwerken

IT-Netze (Informationstechnologie) und OT-Netze (Betriebstechnik, einschließlich Gebäudeleittechnik) weisen Unterschiede in Zweck, Einsatzumgebung und Prioritäten auf. Nachfolgend ein Vergleich dieser beiden Netzwerke:

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:
    - Vertraulichkeit (Schutz der Daten vor unberechtigtem Zugriff)
    - Integrität (Sicherstellung der Richtigkeit und Unverfälschtheit der Daten)
    - 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:
    - Verfügbarkeit (Systeme müssen kontinuierlich laufen)
    - Sicherheit (Vermeidung von Schäden an Menschen und Geräten)
    - Integrität (genaue Kontrolle der physischen Prozesse)

Da die beteiligten Parteien aus den Bereichen IT und Gebäudemanagement häufig unterschiedliche Prioritäten verfolgen, ist eine sorgfältige Abstimmung hinsichtlich der Anforderungen, Cybersecurity-Merkmale sowie der Prioritätensetzung unerlässlich. Im Bereich der Cybersecurity für Gebäudeautomation arbeiten Akteure aus IT und Gebäudesteuerung zusammen, die jeweils spezifische Schwerpunkte bei Sicherheits- und Betriebsanforderungen setzen. Die frühzeitige Identifikation dieser Unterschiede ist von zentraler Bedeutung, um Missverständnisse zu vermeiden.

Für jede einzelne Anforderung sollte eine hauptverantwortliche Person bzw. ein Hauptinteressent benannt werden. Während weitere Stakeholder oder Lieferanten unterstützend mitwirken können, muss die primäre Verantwortlichkeit eindeutig geregelt sein.

6. Cybersecurity-Anforderungen Planen

Diese Sicherheitsgrundsätze für die Erstellung von Gebäudeautomation-Anforderungsspezifikationen orientieren sich an etablierten Leitfäden wie AMEV, VDMA 24774 und dem BSI Cybersecurity Kompendium. Diese Quellen sind für den deutschen Markt ausgelegt, basieren jedoch auf international anerkannten IT-Standards und -Praktiken und können daher auch in anderen Märkten als Referenz dienen. Die Leitfäden behandeln unter anderem folgende Sicherheitsthemen:

- Netzwerke der Gebäudeautomation (Schnittstellen, Fernwartung)
- Absicherung von Komponenten der Gebäudeautomation (Dienste, Konten, Verschlüsselung)

- Passwortrichtlinien (Komplexität, Ablauf, fehlgeschlagene Versuche, automatische Abmeldung, Verlauf)
- Updates, Upgrades und Wartung (Hardware, interne und externe Laptops, Schnittstellen)
- Protokollierung (Benutzeraktionen, Datenänderungen, Umschaltungen sowie Konfigurationsaktionen unter Berücksichtigung datenschutzrechtlicher Vorgaben)

Für die Planung von Gebäudeautomationssystemen werden folgende Grundsätze empfohlen:

- Frühzeitige Einbindung von IT-Sicherheitsaspekten
- Dokumentation und Transparenz des Systems
- Gestaltung sicherer Schnittstellen und Implementierung von Zugangskontrollen
- Regelmäßige Wartung und Aktualisierung des Systems zur Sicherstellung der Leistungsfähigkeit

6.1. Bewertung des aktuellen Zustands

Die Bewertung der Cybersicherheit bestehender Geräte, Anlagen oder Technologien bildet den Ausgangspunkt. Es sollte nicht vorausgesetzt werden, dass die Geräte sicher sind. Häufig ist eine Netzsegmentierung notwendig, um angemessene Sicherheitsanforderungen zu erfüllen.

Welche Merkmale zur Cybersicherheit bietet die vorhandene oder spezifizierte Ausrüstung?

- Unterstützt das Gerät sichere Kommunikationsprotokolle wie verschlüsseltes KNX Secure, BACnet/SC oder OPC UA?
- Wurde überprüft, dass bei vorhandenen Geräten, die verschlüsselte Kommunikation unterstützen, auch die verschlüsselte Kommunikation aktiviert wurde?
- Gibt es in den Spezifikationen Vorgaben zur Inbetriebnahme von sicheren Geräten mit sicheren Protokollen?
- Werden proprietäre Kommunikationsprotokolle verwendet und erfolgt in diesem Fall eine Verschlüsselung der Kommunikation oder wird auf „Security by Obscurity“ gesetzt?
- Kann bei unverschlüsselter Kommunikation das geforderte Sicherheitsniveau durch Netzsegmentierung und IT-Sicherheitsmaßnahmen gewährleistet werden?
- Sind ausreichende Informationen verfügbar, um die Einhaltung der Sicherheitsanforderungen und -richtlinien des Kunden sicherzustellen?
- Wer übernimmt die Bereitstellung und Wartung der IT-Infrastruktur des OT-Netzes und seiner Komponenten?
- Wie werden Passwörter, Sicherheitsschlüssel oder Zertifikate übergeben?
- Welche Maßnahmen bestehen zur Überwachung von Zugriffsrechten auf Passwörter, Projektdaten oder das System selbst?

6.2. Verantwortlichkeiten und Rechenschaftspflicht für Cybersecurity

Für jedes verwaltete System oder jede Gruppe ist eindeutig zu definieren und zu dokumentieren, wer die Verantwortung und wer die Rechenschaftspflicht trägt. Bei bestimmten Aufgaben kann eine weitergehende Klärung erforderlich sein. Verantwortung und Rechenschaftspflicht sind hierbei zu unterscheiden; die verantwortliche Person, beispielsweise der Systemintegrator, unterliegt einer regelmäßigen Berichtspflicht gegenüber der rechenschaftspflichtigen Instanz, meist dem Auftraggeber. Eine klare Kommunikationsstruktur ist unerlässlich, um fundierte Entscheidungen treffen und ein effektives Risikomanagement

gewährleisten zu können – insbesondere im Zusammenspiel mehrerer Parteien wie Gebäudeeigentümern, Mietern oder Organisationen.

Die Begriffe "Verantwortung" und "Rechenschaftspflicht" werden häufig in Verbindung miteinander verwendet, haben aber unterschiedliche Bedeutungen, insbesondere im Management- und Organisationskontext. 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 verantwortlich ist, wenn etwas schief geht.

Beispiel: Der Auftragnehmer ist für das ordnungsgemäße Funktionieren der Gebäudesysteme verantwortlich, auch wenn andere die eigentlichen Arbeiten ausführen.

Rechenschaftspflicht bedeutet, dass man für das Ergebnis verantwortlich ist und bezieht sich in der Regel auf die vertraglich verantwortliche Partei, oft den Installateur und Lieferanten der Gebäudesteuerung.

7. Cybersecurity-Anforderungen an die Gebäudeautomation (GA)

Der BSI-Leitfaden zur Gebäudeautomation (INF.14) richtet sich an Behörden, Unternehmen und Institutionen und liefert praxisnahe Empfehlungen zum Schutz von Daten und Systemen. Das BSI empfiehlt einen ganzheitlichen Ansatz für IT-Sicherheit, der technische, organisatorische und personelle Faktoren einbezieht. Die Richtlinie gilt offiziell für Deutschland, basiert aber auf Standards, die auch international genutzt werden können.

7.1. Grundlegende Cybersecurity Anforderungen (Muss-Anforderungen)

Planung der Gebäudeautomation (GA)

Bei der Planung des Gebäudeautomationssystems ist es zu empfehlen, Cybersecurity-Anforderungen systematisch in den Entwurfs- und Entwicklungsprozess zu integrieren, um ein hohes Maß an Systemsicherheit zu gewährleisten. Der Systementwurf sollte sämtliche GA-Komponenten wie HLK, Beleuchtung, Beschattung sowie Energiemanagement abdecken und dabei auf sichere, standardisierte Systeme und Protokolle setzen. Die kontinuierliche Aktualisierung von Spezifikationen und Zeichnungen ist essenziell für die Aufrechterhaltung der Sicherheit.

Definition und Auswahl von Technologien

Die Anzahl der Automatisierungstechnologien und Subsysteme ist auf Grundlage der vorliegenden Daten zu ermitteln, beispielsweise unter Berücksichtigung der anzuschließenden Anlagen und Geräte, der Verkabelung, der Produktverfügbarkeit sowie des Bedarfs. Zusätzlich sind die erforderlichen Verbindungs- und Kommunikationstechnologien sowie die Einhaltung der rechtlichen und sicherheitstechnischen Anforderungen zu berücksichtigen.

Ausführungsplanung
Die Ausführungsplanung beschreibt den Ablauf der Detailplanung. Sie beinhaltet die Spezifizierung aller erforderlichen Schritte sowie die Festlegung von Zuständigkeiten und Zeitplänen. In der Endabnahmephase wird geprüft, ob die Umsetzung dem detaillierten Plan entspricht und alle Anforderungen erfüllt sind. Abweichungen werden zur weiteren Analyse und gegebenenfalls Korrektur an das Planungsteam gemeldet.

Koordinierung der Gewerke
Koordination aller Gewerke und Beteiligten während des Projekts und der ersten Gebäudenutzung. Festlegung der Reihenfolge zur Inbetriebnahme sowie Integration der Gebäudeeinrichtung in andere Systeme.

Dokumentation der Gebäudeautomation
Alle Komponenten und Zugangspunkte dokumentieren. Dokumentation regelmäßig prüfen und aktualisieren.

Systemsegmentierung und Integration verschiedener Gebäudesysteme und Steuerungssilos
Die Integration isolierter Kontrollsysteme in die Gebäudeautomation sollte sorgfältig geplant und getestet werden, um einen reibungslosen Betrieb sicherzustellen. Es ist darauf zu achten, dass ausschließlich klar definierte Daten und Aktionen zwischen der Gebäudeautomation und den angeschlossenen Systemen ausgetauscht werden.

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

Neben den grundlegenden Anforderungen werden nachfolgend die Kriterien aufgeführt, die dem aktuellen Stand der Technik entsprechen und grundsätzlich in Betracht gezogen werden sollten.

Die folgenden Aspekte sind bei der Planung zu berücksichtigen:

Definition einer Cybersecurity-Richtlinie für die Gebäudeautomation
Die Cybersecurity-Richtlinie für die Gebäudeautomation ist entsprechend der geltenden IT-Cybersecurity-Richtlinien zu erstellen. Die übergeordneten Sicherheitsanforderungen an die Gebäudeautomation und deren Komponenten werden festgelegt, wobei technische Details ausgeklammert werden können. Änderungen und Aktualisierungen sind alsbald den betroffenen Parteien mitzuteilen. Eine nachvollziehbare Dokumentation sowie eine fortlaufende Aktualisierung sind sicherzustellen; zudem muss die Richtlinie sämtlichen relevanten Stakeholdern zur Verfügung stehen.

Spezifikation der Systemarchitektur und deren Auswirkungen auf die Cybersecurity
Die Spezifikationen definieren die Architektur, das Design und die Systemverbindungen der Gebäudeautomation. Die Anforderungsspezifikation erfolgt in zwei Schritten: Zunächst werden die Anforderungen analysiert und strukturiert, anschließend erfolgt die Ausarbeitung der Vorgaben für Gebäudeautomation (GA) sowie technische Gebäudeausrüstung (TGA) mit Kommunikationsschnittstellen. Im Einklang mit den Cybersicherheitsrichtlinien sind vollständige, separate Spezifikationen für die GA, deren Teilsysteme und Nachweise der Gesetzeskonformität unabdingbar. Die zugehörige Dokumentation wird regelmäßig geprüft und im Zuge der Implementierung aktualisiert.

Festlegung eines ganzheitlichen Konzeptes
Für die Gebäudeautomation ist ein umfassendes Konzept zu entwickeln, das die Einhaltung relevanter Cybersicherheitsstandards im laufenden Betrieb sicherstellt. Dieses Konzept umfasst detaillierte Funktions- und Nutzungsstrategien für vernetzte wie auch isolierte Systeme. Zudem sind sämtliche technischen und organisatorischen Anforderungen klar zu benennen und regelmäßig zu überprüfen. Das GA-Konzept bildet die Grundlage für einen sicheren und wirtschaftlichen Betrieb einschließlich technischer Funktionalitäten, Prozessen für den Routinebetrieb und Abläufen bei Systemänderungen und Wartungen. Somit entsteht ein integrierter Rahmen für Planung, Organisation und Technik.

Die Richtlinien, Architekturspezifikation und Nutzungskonzept sollten regelmäßig überprüft und aktualisiert werden, sodass sie den aktuellen technologischen Stand und die geltenden Praktiken abbilden. Dabei gilt es

sicherzustellen, dass das Konzept mit dem bestehenden System übereinstimmt und nicht autorisierte Änderungen identifiziert werden.

Für die technische Umsetzung sind die nachstehenden Aspekte zu berücksichtigen:

Autarkie als Sicherheitsprinzip
Gebäudeautomationssysteme, deren Teilsysteme und Segmente entsprechend dem jeweiligen Schutzbedarf so konzipiert werden, dass sie im Falle eines Ausfalls der primären GA-Verbindung eigenständig und unabhängig funktionieren können. Dabei ist darauf zu achten, kritische Abhängigkeiten von zentralen Steuerungen, anderen Subsystemen oder Segmenten weitestgehend zu minimieren. Bei einer unterbrochenen Verbindung müssen die einzelnen GA-Segmente weiterhin lokal einsatzfähig bleiben. Eine sorgfältige Analyse der Abhängigkeiten zwischen Gewerke und TGA-Anwendungen und angebundenen Systemen ist unerlässlich. Darüber hinaus benötigen einige GA- und IoT-Geräte einen durchgehenden Internetzugang. Sollte ein Gerät ohne Internetverbindung nicht betriebsbereit sein, sind alternative Lösungen oder eine gesicherte, dedizierte Internetanbindung für die Gebäudeautomation zu prüfen.

Standardisierung von Gebäudeautomation -Bereichen für mehr Effizienz und Stabilität
Bereiche mit vergleichbaren Funktionen in der Gebäudeautomation verwenden idealerweise einheitliche technische Lösungen, um Planung und Betrieb zu erleichtern. Jedes Gebäudesegment sollte auch im Falle eines Ausfalls des Hauptsystems eigenständig funktionsfähig bleiben.

Netzarchitektur und Segmentierung
Für die Entwicklung von Gebäudeautomations- und Steuerungssystemen ist eine segmentierte Architektur mit möglichst geringen Abhängigkeiten zwischen den einzelnen Bereichen von zentraler Bedeutung. Auf diese Weise können Segmente unabhängig verwaltet werden, sodass Störungen in einem Teilbereich die übrigen Bereiche nicht oder nur in geringem Maße beeinträchtigen.

Die Segmentierung der Gebäudeautomation erfolgt auf Basis definierter Sicherheitsanforderungen und beginnt mit der Erstellung einer Kommunikationsmatrix, welche das Zusammenspiel aller Komponenten, verwendeten Protokolle und beteiligten Organisationen abbildet. Während die interne Kommunikation innerhalb eines Segments in der Regel uneingeschränkt möglich ist, sollte die Kommunikation zwischen unterschiedlichen Segmenten begrenzt und durch Firewall oder Filterfunktionen abgesichert werden- Zudem ist eine regelmäßige Überprüfung der Segmentierungsstruktur erforderlich.

Zugangskontrollsystem für zentrale oder kritische Gebäudeautomationsgeräte
Ein Zugangskontrollsystem für zentrale oder kritische Gebäudeautomationsgeräte sollte gemäß den Anforderungen der Gebäudeautomation implementiert werden. Dies kann durch spezielle Authentifizierungsmethoden oder über eine Integration in das zentrale IT-System erfolgen. Die Definition von Rollen und Berechtigungen für GA-Operatoren, technisches Personal und Nutzer ist insbesondere bei komplexen Kontrollstrukturen erforderlich. Rollen wie Mieter und Betreiber erhalten spezifisch eingeschränkte Berechtigungen; organisatorische Änderungen werden zeitnah in den entsprechenden Berechtigungen berücksichtigt. Übliche Berechtigungsstufen sind „Nur lesen“, „Lesen/Schreiben“ und „Voller Administrator“, wobei die höchsten Berechtigungen qualifiziertem Personal bei Einrichtung oder wesentlichen Modifikationen vorbehalten sind.

Sichere IP-Kommunikation
Es wird empfohlen, verschlüsselte IP-Protokolle wie z.B. KNXnet/IP Secure oder BACnet/SC einzusetzen. Die Kommunikation mit GA-Netzwerken sollte über ein sicheres Gateway oder eine Systemkomponente mit geeigneter Filterfunktionalität überwacht und eingeschränkt werden. In IP-Netzwerken ist Authentifizierung und Verschlüsselung sicherzustellen, beispielsweise durch TLS 1.3 für BACnet/SC und AES-128-Verschlüsselung für KNX IP Secure. IP-Komponenten mit beschränkten Sicherheits-Eigenschaften sollten überprüft werden. Falls deren weiterer Einsatz notwendig ist, sind diese entsprechend durch Gateways oder Firewalls zu isolieren und zu überwachen; hierbei sind bewährte Verfahren zu berücksichtigen. Bei Nutzung proprietärer Protokolle sollte zudem eine Bewertung der Sicherheit erfolgen.

Sicherheitsmechanismen für Gebäudeautomations-Netzwerke
Sensible Informationen, die nicht über native GA-Protokolle übertragen werden, sollten ausschließlich über HTTPS oder FTPS mit TLS weitergeleitet werden. Der Zugang zum OT-Netzwerk sollte nur für autorisierte

Personen möglich sein. Die Architektur des OT-Netzwerks sollte so gestaltet werden, dass unautorisierte Verbindungen zwischen Segmenten verhindert werden.

Kommunikationsschnittstellen zu externen Systemen
Die Kommunikation zwischen der Gebäudeautomation (GA) und externen Systemen sollte ausschließlich über klar definierte, sichere Schnittstellen stattfinden, die Authentifizierung und Verschlüsselung gewährleisten. Externe Schnittstellen sind auf das notwendige Maß zu begrenzen. Bei einer Anbindung an externe Systeme, wie beispielsweise Gebäudemanagement oder Büro-IT, sind sämtliche Verbindungen und Abhängigkeiten zu dokumentieren.

Verwendung eines dedizierten IP-Adressbereichs für die Gebäudeautomation
Für die Gebäudeautomation sind dedizierte IP-Bereiche eindeutig zu reservieren und von der Büro-IT sowie weiteren Betriebstechnologien (OT) strikt abzugrenzen. Es ist essenziell, eine klare Zuordnung zwischen statischen IP-Adressen und den entsprechenden GA-Komponenten vorzunehmen. Die Vergabe der IP-Adressen sollte nach einem nachvollziehbaren System erfolgen, das sowohl Gebäudestruktur als auch Gerätetypen berücksichtigt. Beim Einsatz von DHCP muss eine sorgfältige Unterscheidung zwischen dynamischen und statischen IP-Adressen getroffen werden, da zahlreiche GA-Geräte fest zugewiesene Adressen benötigen. Eine strukturierte IP-Verwaltung gewährleistet eine konsequente Trennung, Transparenz und eine optimierte Administration.

Broadcast-Kommunikation
In IT-Netzwerken empfiehlt es sich, den Broadcast-Verkehr zu reduzieren, um eine Netzüberlastung zu vermeiden. Unicast- oder Multicast-Kommunikation sind vorzuziehen; Broadcasts sollten nur bei explizitem Bedarf eingesetzt werden. GA-Router können meist so konfiguriert werden, dass sie Broadcasts nur weiterleiten, wenn dies erforderlich ist.

Anzeige der Gültigkeit der Werte
Fernüberwachte Gebäudeleitsysteme müssen eindeutig erkennen, ob die angezeigten Daten, wie Werte oder Statusinformationen, aktuell sind. Das System sollte veraltete kritische Daten erkennen und entweder eine Benutzerbenachrichtigung ausgeben oder eine definierte Fehlerreaktion initiieren, um Bewohner und Gebäude zu schützen. Simulierte oder “eingefrorene” Daten sollten im Bedarfsfall gekennzeichnet oder durch einen Alarm angezeigt werden.

Gebäudeautomationssysteme, ihre Teilsysteme und Segmente sollten entsprechend dem jeweiligen Schutzbedarf so konzipiert werden, dass sie im Falle eines Ausfalls der primären GA-Verbindung eigenständig und unabhängig funktionieren können. Dabei ist darauf zu achten, kritische Abhängigkeiten von zentralen Steuerungen, anderen Subsystemen oder Segmenten weitestgehend zu minimieren. Im Falle einer unterbrochenen Verbindung müssen die einzelnen GA-Segmente weiterhin lokal einsatzfähig bleiben. Eine sorgfältige Analyse der Abhängigkeiten zwischen Steuerungssilos, Geräten und angebundenen Systemen ist unerlässlich. Darüber hinaus benötigen einige GA- und IoT-Geräte einen durchgehenden Internetzugang. Sollte ein Gerät ohne Internetverbindung nicht betriebsbereit sein, sind alternative Lösungen oder eine gesicherte, dedizierte Internetanbindung für die Gebäudeautomation zu prüfen.

Robuste Komponenten
In anspruchsvollen Umgebungen sollten entweder langlebige Komponenten eingesetzt werden oder gegebenenfalls alternative Maßnahmen angewendet.

Zeitsynchronisierung
Automatisierte Messungen, Steuerungen und Regelungen in der Gebäudeautomation sollten mit synchronisierter Zeit arbeiten. Für Echtzeitkommunikation im GA-System werden GA-eigene Methoden zur Zeitsynchronisation empfohlen, statt ausschließlich NTP zu nutzen.

Statusprotokolle
Das Protokollieren sicherheitsrelevanter Laufzeitereignisse sowie der Geräteverfügbarkeit ist für GA-kritische Systeme zwingend erforderlich. Hierzu ist die Erstellung und Umsetzung eines geeigneten Überwachungsplans notwendig. Die Verfügbarkeit und relevante Schlüsselparameter sind kontinuierlich zu überwachen. Fehlerfälle oder Grenzwertüberschreitungen werden automatisch der zuständigen Betriebsorganisation gemeldet. Bei Systemausfällen oder Einschränkungen in der Kontrollfunktion erfolgt eine automatisierte

Alarmierung. Es wird definiert, welche Ereignisse entsprechende Alarme auslösen. Statusberichte und Überwachungsdaten werden ausschließlich über sichere Kommunikationskanäle übertragen. Feldgeräte wie KNX-Systeme unterliegen einer Überwachung und sollten Funktionen zur regelmäßigen Statusmeldung vorsehen. Geräte auf Automatisierungs- oder Managementebene übernehmen die zentrale Überwachung und lösen bei Bedarf entsprechende Alarme oder Benachrichtigungen aus.

Änderungsprotokolle
Neben der Protokollierung von Statusänderungen an Komponenten der Gebäudeautomation ist auch die Erfassung sicherheitsrelevanter Ereignisse erforderlich. Sämtliche Konfigurationsänderungen an gebäudetechnischen Systemen, für die Gebäudeautomation relevante Komponenten sowie sämtliche manuellen oder automatisierten Zustandsänderungen – einschließlich Software- oder Firmware-Updates – sind zu dokumentieren. Es sollte festgelegt werden, welche Protokolldaten zentral gespeichert werden. Da Änderungen sowohl Verdrahtungen, physische Modifikationen als auch Anpassungen mittels externer Tools umfassen können, ist eine direkte Protokollierung von GA-Änderungen nicht immer möglich. In solchen Fällen können Inbetriebnahme- und Standortberichte von Installateuren, Wartungspersonal und Systemintegratoren als ergänzende Dokumentationsquellen herangezogen werden.

Notfallplanung
Regelmäßige Überprüfung der Auswirkungen von Gebäudeautomation auf die Notfallplanung. Entwicklung von Richtlinien zur Reduzierung möglicher Unterbrechungen durch Ausfälle der Gebäudeautomation infolge technischer Störungen oder Cyberangriffen. Die Notfallpläne sollten Kontaktinformationen für das Wartungspersonal sowie für im Notfall zuständige Personen enthalten. Verfahren zur Sicherstellung wesentlicher Betriebsabläufe bei Ausfällen der Gebäudeautomation und Dokumentation von Plänen für den Wiederanlauf sind festzulegen.

7.3. Anforderungen für kritische Systeme mit erhöhten Anforderungen an die Cybersicherheit

Erwägen Sie zusätzliche Anforderungen für einen höheren Schutz auf der Grundlage einer Risikobewertung.

Dediziertes physisches Netzwerk für die Gebäudeautomation
Um den Schutz zu gewährleisten, empfiehlt es sich, sicherheitsrelevante GA-Netze physisch von anderen Netzwerken zu trennen. Verbindungen zu externen Cloud-Diensten sollten über spezielle, kontrollierte Internetzugänge erfolgen. Ebenso sind Zugriffe auf nicht vertrauenswürdige Netzwerke, einschließlich interner Bürobereiche, gemäß den GA-Schutzanforderungen zu blockieren.

8. Ein störungsresistentes GA-System ist auch gegen Cybersecurity-Risiken gut gewappnet.

Die erste Schutzmaßnahme gegen Cybersicherheitsbedrohungen ist ein sorgfältig konzipiertes und fehlertolerantes Gebäudeleitsystem. Bei einer angemessenen Segmentierung entstehen keine zentralen Fehlerpunkte; stattdessen sind die Kontrollfunktionen verteilt und möglichst lokal organisiert. Dieser Ansatz reduziert die potenziellen Schwachstellen und beeinflusst die Sicherheit von Automatisierungslösungen wie beispielsweise KNX-Systemen. Eine robuste Segmentierung und dezentrale Kontrolle kann das Risiko von Cyberangriffen deutlich senken.