/SSS information security society switzerland

Gebäudesicherheits-Check:
Büros & Öffentliche Gebäude

Die Steuerung von Gebäudefunktionen wie Heizung, Strom, Wasser, Transport (z.B. Lifte), Sicherheit (Sicherheits- und Zutrittskontrollsysteme Einbruchmelde- und Überwachungssysteme) und Belüftung ist ein unverzichtbarer Bestandteil moderner Gebäude.

Diese Systeme, häufig unter den Begriffen Domotik oder Gebäudeautomation bekannt, erfüllen zentrale Funktionen innerhalb eines Gebäudes. Mit der fortschreitenden Vernetzung dieser Systeme und besonders mit ihrer voranschreitenden Integration ins Internet entstehen neue Risiken.

Ein Cyberangriff auf solche Systeme kann nicht nur den Betrieb des Gebäudes beeinträchtigen, sondern im schlimmsten Fall auch Menschenleben gefährden.

Information Security Society Switerland (ISSS),
Zentweg 13, 3006 Bern

info@isss.ch isss.ch

Ziel und Zweck des Dokuments

Dieses Dokument dient als Hilfestellung für Projektleiter & Betreiber von Gebäuden, mit Fokus auf kritische Infrastrukturen und öffentliche Gebäude (Schulen, Spitäler, öffentliche Verwaltung, etc.). Es bietet praxisorientierte Empfehlungen und Best-Practices zur Implementierung von Sicherheitsmassnahmen.

Das Dokument soll in der Projektierungsphase eines neuen Gebäudes Orientierung bieten, damit Cybersecurity von Beginn an in die Planung integriert wird. Ziel ist es, die Integrität und Verfügbarkeit von Systemen zu gewährleisten, die für den Betrieb dieser Einrichtungen entscheidend sind. Eine vorgängige Risikoanalyse und/oder Threat Model ist empfohlen, um die kritischen Systeme und Bedrohungen zu identifizieren.

Wie kann ich diese Massnahmen umsetzen

Es bestehen drei Möglichkeiten, wie die Massnahmen umgesetzt werden. Erstens und die empfohlene Methode, bildet die eigenständige Umsetzung. Somit wird auch der Know-How Aufbau in der Organisation selbst sichergestellt. Zweitens, in Zusammenarbeit mit dem Dienstleister. Denn letzterer kennt die Systeme im Detail. Drittens, mit einem Beratungsunternehmen seines Vertrauens. Denn diese verfügen oftmals über umfangreiche Erfahrung mit Cybersecurity im Domotik-Bereich.

Rollen und Verantwortlichkeiten

Die Verantwortung für Cybersecurity soll klar definiert werden, das sowohl in der Projektierung als auch im Betrieb die Sicherheit gewährleistet wird. Risiken müssen identifiziert und angemessen behandelt werden. Sie sollten in das Risikomanagement des Projekts und Betriebs integriert werden.

Im Projekt: Der Projektleiter

Der Projektleiter muss in der Planungsphase darauf achten, dass die Gebäudeautomation sicher konzipiert und später auch sicher betrieben werden kann:

- In der Planungsphase trägt der Projektleiter eine zentrale Verantwortung dafür, dass die Gebäudeautomation von Anfang an unter strengen Sicherheits- und Zuverlässigkeitsaspekten konzipiert wird. Dies umfasst nicht nur die sorgfältige Auswahl geeigneter Technologien, sondern auch die Schaffung passender organisatorischer Rahmenbedingungen, den Einbezug qualifizierter Fachkräfte sowie die konsequente Anwendung anerkannten Normen und bewährter Best Practices für Domotik-Systeme.
- Bereits in der ersten Planungsphase sollte der Projektleiter wo möglich und sinnvoll IT-Sicherheitsexperten und Fachplaner für Gebäudeautomation involvieren. Deren Input ist entscheidend, um potenzielle Risiken und Schwachstellen frühzeitig zu erkennen und angemessen zu adressieren.

Im Betrieb: Der Gebäudebetreiber

Die Systeme erfordern Wartung & Updates und der Fernzugriff von verschiedenen Parteien muss überwacht werden. Eine verantwortliche Person im Betrieb (Bsp. Technischer Dienst) ist notwendig, um sich um diese Aufgaben zu kümmern. Es muss sichergestellt werden, dass diese Person über ausreichend zeitliche und finanzielle Ressourcen verfügt, um dieser Verpflichtung nachzukommen, sowie ein gewisses technisches Know-How mit sich bringt oder aneignet.

Eine enge Zusammenarbeit mit der IT-Abteilung/IT-Spezialisten ist erstrebenswert, wenn es um TCP/IP Themen und insbesondere der Netzwerkkonfiguration und das Management der externen Zugriffe geht. Um den Betrieb sicherzustellen, sollten ausserdem regelmässig Schulungen und Sensibilisierungsmassnahmen sichergestellt werden. Auch Ausfallszenarien für den Ernstfall sollten geübt werden (BCM-Übung).

Anforderungen & Hilfestellungen

Die folgenden Unterkapitel bieten pragmatische Hilfestellungen für den sicheren Aufbau und Betrieb der Gebäudeautomationsinfrastruktur. Es werden primär jene technischen und organisatorischen Massnahmen dargestellt, welche als Minimalschutz der Domotik in Betracht gezogen werden sollen.

Es ist ein Massnahmenpaket, dass wenn korrekt umgesetzt, mit verhältnismässig wenig Aufwand einen guten Ertrag, respektive Risikoreduktion entsprechend dem Paretoprinzip liefert. Das Dokument kann auch für bereits in Betrieb stehende Gebäude als Orientierung verwendet werden, um diese im Nachinein besser vor Angriffen zu schützen.

Die Massnahmen sind unterteilt in zwei Stufen: **Essenziell (Tier 1)** und **Empfehlenswert (Tier 2).**

Essenzielle Anforderungen (Tier 1)

Die folgenden Anforderungen stellen aus Sicht des ISSS eine nachdrückliche Empfehlung dar. Sie definieren die minimal erforderlichen Sicherheitsmassnahmen, welche umgesetzt werden sollen.

Inventar

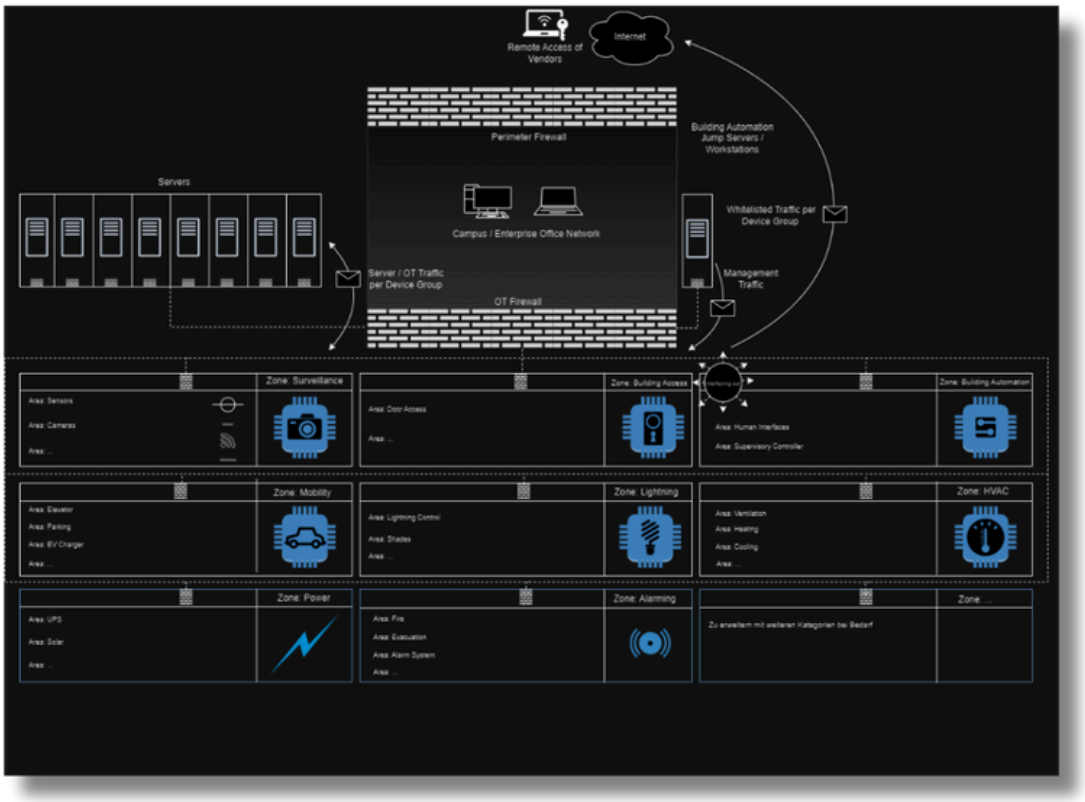
Herausforderung:

- Oftmals besteht kein vollständiges und aktuelles Inventar aller Geräte und Systeme in der Gebäudeautomation. Dies führt zu einer unzureichenden Sichtbarkeit und Kontrolle über potenzielle Sicherheitsrisiken.

Lösungsansatz:

- Führen Sie ein Inventar aller Geräte, Systeme und Softwareanwendungen in der Gebäudeautomation. Nutzen Sie automatisierte Tools zur Erfassung und Aktualisierung des Inventars regelmässig, um sicherzustellen, dass alle Komponenten erfasst und bewertet werden. Falls kein Tool zur Verfügung steht, verwenden Sie eine Excel-Liste.

Netzwerkarchitektur / Zonierung



Das Musterschema (Grafik oben) zeigt, wie ein Gebäudebetreiber seine OT-Geräte für Gebäudeautomation im Netzwerk platzieren und segmentieren kann, angelehnt an das Purdue-Modell, aber pragmatischer umgesetzt. Geräte sollten in funktionale Kategorien unterteilt und durch VLANs sowie Firewalls sauber getrennt werden, um eine sichere Kommunikation zu gewährleisten. Internetzugriffe müssen strikt nach dem Whitelisting-Prinzip geregelt sein, und Remotezugriff sollte nur on-demand erfolgen. Für das Management empfiehlt sich ein dedizierter Server, der isoliert vom produktiven Netzwerk betrieben wird.

Herausforderung:

- Eine unzureichend segmentierte Netzwerkarchitektur kann dazu führen, dass Angreifer leicht von einem Gerät zum anderen gelangen und kritische Systeme kompromittieren.

Lösungsansatz:

- Implementieren Sie eine segmentierte Netzwerkarchitektur, die kritische Systeme von weniger sicheren Bereichen trennt. Verwenden Sie Firewalls und VLANs, um den Datenverkehr zu kontrollieren und den Zugriff auf sensible Bereiche zu beschränken. Das Gebäudeautomationssystem sollte von der Büroautomation / Produktionssystemen getrennt sein.

Netzwerkverkehr mit Whitelisting regeln

Herausforderung:

- Unkontrollierter Netzwerkverkehr kann zu Angriffen führen, da böswillige Aktivitäten nicht erkannt werden.

Lösungsansatz:

- Implementieren Sie ein Whitelisting für den Netzwerkverkehr (z.B. mit Hilfe einer Firewall), um nur autorisierte Geräte und Anwendungen zuzulassen. Überwachen Sie den Netzwerkverkehr kontinuierlich, um verdächtige Aktivitäten zu identifizieren und zu blockieren.

Zugriffsmanagement & Sichere Grundkonfiguration

Herausforderung:

- Unzureichendes Zugriffsmanagement kann dazu führen, dass unbefugte Benutzer Zugriff auf kritische Systeme erhalten, was zu Datenverlust oder -beschädigung führen kann.
- Systeme kommen häufig mit suboptimalen Grundkonfigurationen, welche sich negativ auf den optimalen Schutz der Komponenten auswirken kann.

Lösungsansatz:

- Stellen Sie sicher, dass Standardpasswörter geändert sind und nur jene Funktionen in Betrieb gesetzt sind, welche für Ihren Use Case auch wirklich benötigt werden.
- Implementieren Sie ein strenges Zugriffsmanagement, das auf dem Prinzip der geringsten Privilegien (least priviledge) basiert. Verwenden Sie wo möglich Multi-Faktor-Authentifizierung (MFA) und regelmässige Überprüfungen der Zugriffsrechte, um sicherzustellen, dass nur autorisierte Benutzer Zugriff auf kritische Systeme haben. Stellen Sie ausserdem sicher, dass kein direkter Zugriff sondern ein sicherer Zugriff (z.B. über VPN oder Jump Host) besteht. Ausserdem sollte ein Prozess bestehen, durch welchen das User-Management (Joiner-Mover-Leaver) adressiert wird.
- Implementieren Sie ein Backup, welches zumindest die Konfiguration des Systems zur Gebäudeautomation umfasst. Bei jeder Konfigurationsänderung soll eine Kopie der Konfiguration erstellt werden (z.B. auf einen offline Speicher), um für eine Wiederherstellung vorbereitet zu sein.

Empfohlene Anforderungen (Tier 2)

Es folgen Vorschläge für zusätzliche aus Sicht des ISSS grundlegende Massnahmen, die das Gesamtsicherheitskonzept optimieren. Sie dienen als Orientierung, um bei ausreichenden Ressourcen und Möglichkeiten weitere Sicherheitsvorkehrungen umzusetzen.

Kommunikationsmatrix & Protokoll Best-Practices

Herausforderung:

- Fehlende oder veraltete Kommunikationsprotokolle zwischen den Geräten können zu Sicherheitslücken und ineffizienten Reaktionen auf Vorfälle führen. Oftmals ist keine Verschlüsselung des Traffic möglich.

Lösungsansatz:

- Erstellen Sie eine Kommunikationsmatrix, die alle Kommunikationswege zwischen den Geräten und Systemen dokumentiert. Definieren Sie klare Protokolle und Sicherheitsanforderungen für jede Verbindung, um sicherzustellen, dass alle Datenübertragungen sicher sind. Verwenden sie moderne Protokolle (z.B. BACnet/SC, KNX Secure, OPC UA) bei neuen Projekten.

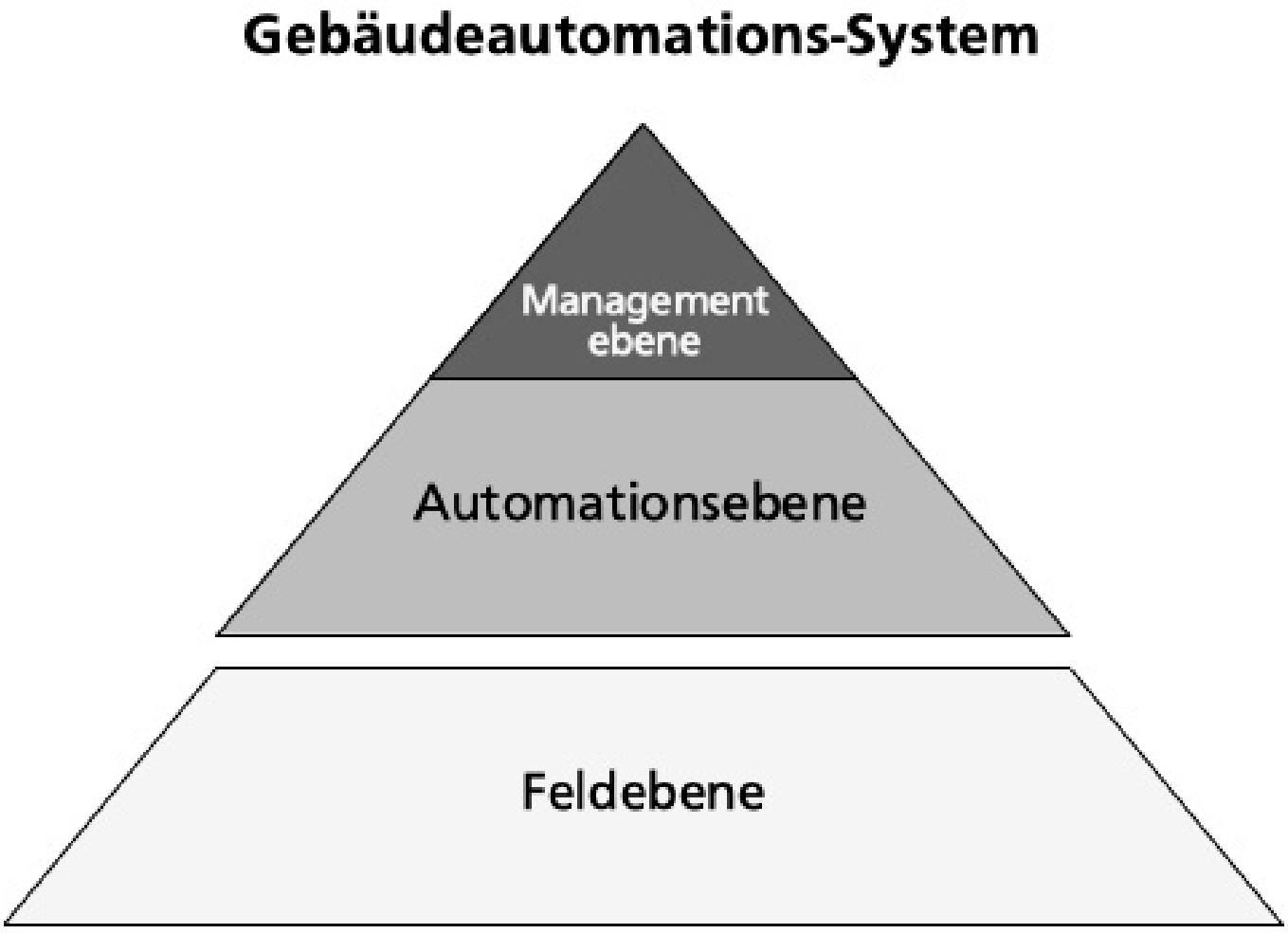
Patchmanagement

Herausforderung:

- Systeme zur Gebäudeautomation sind oft für einen langen Lifecycle (mehrere Dekaden) konzipiert und können nicht oder nur unzureichend gepatched werden. Unzureichendes Patchmanagement kann dazu führen, dass bekannte Sicherheitsanfälligkeiten in Geräten und Software nicht behoben werden.

Lösungsansatz:

- Es sollten nur verifizierte Patches des Herstellers verwendet werden.
- Entwickeln Sie einen strukturierten Patchmanagement-Prozess, der regelmässige Überprüfungen und zeitnahe Updates für alle Systeme und Geräte umfasst. Automatisieren Sie den Patchprozess, wo immer möglich, um sicherzustellen, dass alle Sicherheitsupdates zeitnah angewendet werden.
- Konzentrieren Sie sich dabei auf die „obereren“ IP-Systeme (jene, die direkt in das Unternehmensnetzwerk eingebunden ist), falls das Gebäudeautomationssystem (siehe Grafik), als Ganzes, selbst nicht gepatched werden kann. Diese Komponenten sind häufig am exponiertesten und bieten daher den grössten Angriffsvektor.



Backup

Herausforderung:

- Fehlendes Backup kann dazu führen, dass das betroffene System nicht mehr oder nur erst nach langer Wiederherstellungszeit wieder läuft.

Lösungsansatz:

- Erstellen Sie ein Recovery-Konzept, das die Wiederherstellung ihrer Systeme Schritt für Schritt erklärt. Optional (Wenn möglich): Testen Sie die Wiederherstellung regelmässig, um sicherzustellen, dass die Systeme im Notfall schnell und zuverlässig wiederhergestellt werden können (z.B. in Zusammenarbeit mit dem Hersteller). Kritische Systeme sollten redundant konzipiert und aufgebaut werden, wenn möglich. Diese Redundanzsysteme sowie die Redundanzen selbst (z.B. durch Failover-Test) sind regelmässig zu testen.

Mitglieder ISSS-Taskforce Domotik

Leitung		Mitglieder	
Arie Malz	President	Samuel Bärfuss	CEO at KOCH IT AG & ISPIN AG
Dario Walder	Vice President ISSS	Lukas Merz	Consultant Redguard
Andrea Michel	Geschäftsstellenleiterin ISSS	Stefan Merz	Head of Consulting United Security Providers AG
Bernhard Tellenbach	Head of Cyber Security, armasuisse W+T	Reto Kaeser	vCISO astarios
		Eduardo Geraldi	CISO & DPO (Director) SPIE Switzerland
		Dario Stöckli	CISO, Aebi Schmidt Group
		Thorsten Ziercke	Strategischer Berater Zirecke Digital Consulting
		Michael Mäder	Professor HES-SO Haute école spécialisée de Suisse occidentale
		Nadri Mamuti	Managing Consultant for Digital Business, Eraneos
		Giorgio Tresoldi	Senior Architect Defense & Intelligence, IBM