

IT-Sicherheit in der Gebäudeautomation

White Paper

Dokumentnummer: D100229513

Revision: 02

Version: 02



2021 © Fr. Sauter AG

Im Surinam 55

4058 Basel

Schweiz

Tel.: +41 61 – 695 55 55

Fax: +41 61 – 695 55 10

www.sauter-controls.com

info@sauter-controls.com

Dokumentnummer: D100229513

Revision: 02

Version: 02

Inhaltsverzeichnis

Inhaltsverzeichnis	3
Änderungsverzeichnis	4
Abbildungsverzeichnis	5
Symbolverzeichnis	6
1 Zusammenfassung (Executive Summary)	7
2 Einleitung/Allgemeines	9
3 Die Elemente der IT-Sicherheit in der GA	11
3.1 Elemente auf Herstellerebene	13
3.2 Zugangsrechte-System / Passwortschutz	15
4 Schlussbemerkung	29
5 Literatur- /Quellenverzeichnis	31
Abkürzungsverzeichnis	32
6 32	
7 Index	33

Abbildungsverzeichnis

Abb. 1: Bereiche und Netzwerke des GA-Systems	11
Abb. 2: Massnahmen nach Zuständigkeitsebene	13
Abb. 3: Bedrohungen und Gegenmassnahmen der IT-Sicherheit für die GA	27

Symbolverzeichnis

**Information**

Für die Handhabung mit dem Produkt relevante Informationen.

**Handlungsaufforderung**

Der Leser wird zum Handeln aufgefordert.

**Internetlink**

Verweise auf Links oder Anwendungen im Internet.

**Warnhinweis**

Warnhinweise stehen vor der Handlung.

Struktur**Art und Quelle der Gefahr**

Folgen

► Massnahmen

1 Zusammenfassung (Executive Summary)

Das Thema IT-Sicherheit in der Gebäudeautomation (GA) ist keine Wunschvorstellung mehr, die man einfach umgehen kann. Die Umgebung hat sich in den letzten Jahren radikal geändert. Neben der allgemeinen Zugänglichkeit der GA-Lösungen über das Internet haben zwei weitere massive Änderungen in den letzten Jahren stattgefunden. Einerseits hat die Virtualisierung der Applikationen und die Auslagerung in die Cloud zu neuen Lösungen aber auch neuen Teilnehmern geführt. Andererseits hat das rasante Wachstum des IoT „Internet of Things“ zu unglaublichen Mengen von neuen Geräten und Daten, die den Bedarf nach Internet-Kommunikation und Zugang zu Cloud-Services exponentiell erhöht.

Wo vor kurzem die GA als isolierte Lösung betrachtet werden konnte, ist jetzt die volle Integration mit vielen anderen Gewerken und Geräten notwendig. Diese bringen auch eine Änderung des Verhaltens und der Erwartungen der Nutzer mit sich. Alles zusammen führt zu einer Vermehrung von Angriffsmöglichkeiten für die Cyberkriminelle.

Im Unterschied zur allgemeinen IT sind bei der Gebäudeautomation dabei mehr als „nur“ Daten bedroht. Wegen der physischen Verbindungen der GA mit den technischen Einrichtungen des Gebäudes (Lüftung, Licht, Türen, Zutrittssysteme) haben Angriffe auch das Potential sicherheitsrelevanter Folgen am Gebäude selbst.

Das tatsächliche Risiko jedes Gebäudes ist projektspezifisch und stark abhängig von dessen Sensibilität und der Wirkungstiefe der GA.

Für den Schutz eines GA-Systems kommen prinzipiell Massnahmen auf drei Ebenen zur Anwendung: Schutz der einzelnen Geräte/PC/Softwares, Schutz der IT Infrastruktur, d.h. der Netzwerke und der Netzwerkzugänge und letztens Massnahmen in den Prozessen.

Die Anwendung von Schutzmassnahmen für die Geräte/PC/Softwares beginnt bereits beim Hersteller. IEC 62443-3-3 bietet eine Liste von Anforderungen, auf denen die Hersteller Lösungen anbieten sollen. Die Schutzmassnahmen für die IT Infrastruktur und die Komplettierung jener für die Geräte/PC/Softwares liegen beim Anlagenersteller, wobei die Auftraggeber, Bauherren und Fachplaner mit ihren Ausschreibungen und Leistungsverzeichnissen den Rahmen, insbesondere den Kostenrahmen dafür vorgeben. Hierfür gibt es sowohl internationale Standards (IEC-62443, u. a.) wie auch Empfehlungen von nationalen Verbänden, besonders für kritische oder strategische Anlagen.

Die Anstrengungen für die IT-Sicherheit erstrecken sich über den gesamten Werdegang einer Anlage, vom Hersteller der Komponenten, über die Projektierung, die Inbetriebsetzung, bis zur Wartung und den Betrieb. Ein adäquater Sicherheitsstandard kann nur erreicht werden, wenn alle beteiligten Instanzen ihren geforderten Beitrag dazu leisten. Die Sicherheitsvorkehrungen müssen den Risiken angepasst werden. Eine Risikoanalyse ist unerlässlich.

Dieses White Paper «IT-Sicherheit in der Gebäudeautomation» gibt einen Überblick über die möglichen Schutzmassnahmen im Einzelnen. In den Grafiken finden sich zusätzlich Informationen über die verschiedenen Bedrohungen. Für einen systematischen Ansatz wird die Norm IEC 62443 empfohlen. Lokale Empfehlungen oder Regelungen sind auch zu beachten. Der Einsatz von spezialisierten Fachleuten wird empfohlen.

Das White Paper behandelt ausschliesslich den Anteil IT-Sicherheit gegen unerwünschten Eingriff/Angriff von aussen. Den Aspekt der IT-Verfügbarkeit und jener der technischen Sicherheit der HLK-Anlage selbst, wird höchstens insoweit angesprochen, als dies einer Schadensminderung beim Ausfall der Steuerung dient.

2 Einleitung/Allgemeines

Dieses White Paper mit dem Titel IT-Sicherheit in der Gebäudeautomation behandelt ausschliesslich den Anteil IT-Sicherheit gegen unerwünschte Eingriffe/Angriffe von aussen. Den Aspekt der IT-Verfügbarkeit (sicher im Sinn von fällt nie aus, stürzt nie ab, Redundanz...), der oft auch als Bestandteil dieses Themas angesehen wird, wird hier nicht betrachtet. Auch der Aspekt der Sicherheit der HLK-Anlage selbst (z.B. Notstromversorgung, Hardwareverriegelungen, Redundante Ausführung von Anlageteilen...) wird hier höchstens insoweit angesprochen, als er bei einem Ausfall der Steuerung der Schadensminderung dient.

Der Auslöser für die wachsende Bedeutung und die Aktualität des Themas IT-Sicherheit in der Gebäudeautomation liegt in der technologischen Entwicklung. In der gesamten Automatisierungstechnik wird seit längerer Zeit immer mehr Intelligenz in immer tiefere Ebenen verbaut. SPS und Automationsstationen haben sich längst zu branchenspezifischen Kleinstcomputern mit eingebettetem Betriebssystem entwickelt. Für die Kommunikation wurden als Folge weitgehend die bestehenden Technologien der allgemeinen IT übernommen. Auch bei den Feldgeräten hält der Trend zu immer mehr integrierter Intelligenz und immer höherwertigen Kommunikationstechniken an. Ähnlich wie in der Raumbedienung, wo sich private Mobilgeräte (BYOD) oder neue Bedienkonzepte mit Sprachassistenten (z.B. Amazon Alexa!, Google Hello, etc) durchgesetzt haben. Diese neue Lösungsansätze (Cloud, KI) verlangen zusätzliche Schnittstellen und Protokolle (WiFi^{TM1}, Bluetooth^{®2}, LoRaWAN^{®3}, Web-API, MQTT, OPC, uvm.) welche zusätzliche Angriffsmöglichkeiten bieten.

In der Gebäudeautomation (GA) war die Entwicklung der letzten ca. 10, 15 Jahre darüber hinaus geprägt von Standardisierung und Öffnung. Die Integrationsfähigkeit der Systeme verschiedener Hersteller wurde zu einem wichtigen Verkaufsargument. Während die Systeme zuvor in jeder Hinsicht proprietär aufgebaut waren und damit kaum oder nur schwierig miteinander kommunizieren konnten, wurden um die Jahrtausendwende Standards auf Netzwerk-, Protokoll- und Objektebene definiert und die Systeme damit geöffnet.

Durch die Nutzung allgemeiner IT-Standards für die Kommunikation, wurde die Integration der Gebäudeautomation in die bestehenden Strukturen der Business-IT eines Gebäudes ermöglicht. Für die Fernkommunikation hat sich die Nutzung des Internets etabliert, womit sich der GA fast unbegrenzte Kommunikationsmöglichkeiten eröffnet haben.

All diese Modernisierungen haben den Kunden und Betreibern der Gebäudeautomation riesige Mehrwerte in Form von immer besseren

¹ Wi-Fi[®], the Wi-Fi logo, the Wi-Fi CERTIFIED logo, and other marks are trademarks of Wi-Fi Alliance.

² © 2021 Bluetooth SIG, Inc

³ LoRa, LoRaWAN[®], Copyright © 2021 LoRa Alliance[®]

Funktionalitäten, von fast unbegrenzten Kommunikationsmöglichkeiten und von völliger Wahlfreiheit bei Neu- und Erweiterungsprojekten beschert.

Mit diesen an sich erfreulichen Entwicklungen hat sich die GA jedoch auch eine neue Dimension der Verwundbarkeit eingehandelt. Diese ist heute weitgehend identisch mit jener der allgemeinen IT.

Durch die physische Verbindung der GA mit den technischen Einrichtungen eines Gebäudes (HLK-Anlagen, Beleuchtung, Zutrittskontrolle, Feuertüren etc.) ergibt sich jedoch, gegenüber der allgemeinen IT, eine erweiterte Dimension bei den Folgen dieser Verwundbarkeit. Nicht „nur“ Daten können manipuliert oder geändert werden, ein unerwünschter Zugriff kann sich bis hin zu den sicherheitsrelevanten technischen Einrichtungen des Gebäudes auswirken. Bei krimineller Absicht können die Folgen entsprechend schwerwiegend sein.

Die Bedeutung der Verwundbarkeit hängt stark vom Typ und der Nutzung des betroffenen Gebäudes ab. Nicht alle Gebäude sind gleich interessant für Angriffe und gleich sensibel für deren Folgen.

Sind bei der Gebäudeautomation „nur“ HLK (Heizungs- Lüftungs- und Kälte-) Gewerke auf-geschaltet, werden sicherlich geringere Risiken zu erwarten sein, als wenn auch Licht, Zutrittskontrolle, Türsteuerungen etc. mit aufgeschaltet sind. Auch ist klar, dass das Risiko bei kleineren nicht öffentlichen Gebäuden nicht dasselbe ist, wie bei zentralen, stark frequentierten, oder besonders sicherheitssensiblen Gebäuden (Flughäfen, Bahnhöfen...). Bei diesen Gebäuden könnte die Absicht der Bedrohung im Extremfall bis hin zu digital unter-stützten Gewaltakten oder Terroranschlägen reichen.

Die Sicherheitsvorkehrungen müssen dem Risiko angepasst sein. Eine projektspezifische Risikoanalyse ist in jedem Fall unerlässlich.

Fundamentale Massnahmen sollten in allen Anlagen vorgesehen werden. Hier ist eine Strategie der Verteidigung in der Tiefe (Defense-in-depth), also der Einsatz von mehreren Schutzmassnahmen und Schutztechnologien generell empfohlen. Eine Maximierung der Sicherheit ist jedoch nur mit sehr grossem Aufwand zu erreichen. Eine absolute, 100prozentige Sicherheit ist auch in der Gebäudeautomation selbst mit dem grössten Auf-wand kaum möglich.

3 Die Elemente der IT-Sicherheit in der GA

Die Sicherheit der netzwerkbasierenden Gebäudeautomation (GA) kann mit Schutzmassnahmen auf prinzipiell zwei Ebenen verbessert werden:

Analog dazu, wie die Bewohner einer mittelalterlichen Stadt durch die Sicherung ihrer Haustüren und/oder durch die Sicherung der Stadttore geschützt werden konnten, können für die GA die Schutzmassnahmen bei den einzelnen Geräten (Automationsstationen, PCs, etc.) und/oder bei den Zugängen der betroffenen Netzwerke getroffen werden. Und wie es damals sicher besser war, die Gefahr gar nicht erst in die Stadt zu lassen und die Stadttore gut zu sichern, ist auch bei der GA der Schutz der Netzwerkzugänge der wohl wichtigere Anteil. So wie aber auch Stadttore und -mauern nie 100% dicht sein können und ausserdem gefährliche Subjekte auch von innerhalb der Stadt kommen können, ist genauso auch der Schutz der einzelnen GA-Geräte unerlässlich.

Ein gutes Resultat kann nur durch Anstrengungen auf beiden Ebenen zusammen erreicht werden.

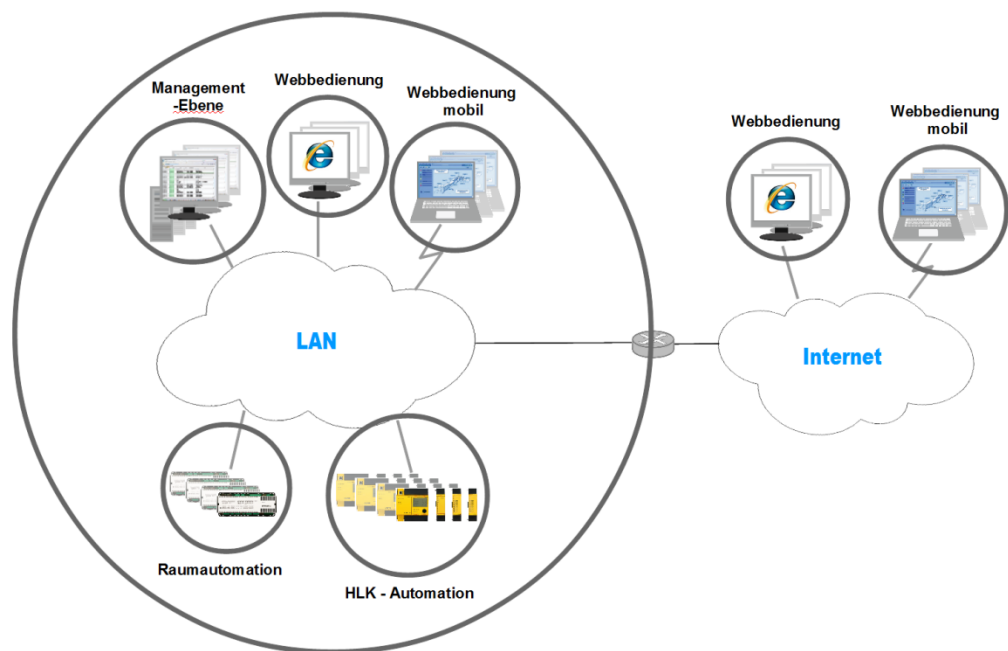


Abb. 1: Bereiche und Netzwerke des GA-Systems

Im Werdegang einer GA-Anlage beginnen die Massnahmen auf der Ebene der einzelnen Geräte/Softwares bereits beim Produktheersteller. Er integriert schon ab Werk möglichst umfassende Sicherheitsmassnahmen in seine Produkte. Z.B. ein Zugriffsrechtssystem mit Passwortschutz, die Unterstützung verschlüsselter Kommunikation, interne Firewalls usw.

Diese vorinstallierten Schutzmassnahmen auf Ebene der Geräte/Software müssen nach-folgend bei der Anlageerstellung und -inbetriebnahme weiter komplettiert und parametrieren werden. Das Zugriffsrechtssystem muss eingerichtet, die Default-Benutzer entfernt, die Geräte evtl. nachgehärtet werden. Die zugekauften PCs müssen in dieser Phase mit einem Malwareschutz (Antivirusprogramm) ausgestattet und auch so weit wie möglich nachgehärtet werden.

Auf die Massnahmen auf Ebene der IT-Infrastruktur, d.h. der Netzwerke/Netzwerk-segmente und deren Zugänge hat der GA-Hersteller üblicherweise kaum mehr, oder nur noch indirekten Einfluss. Diese werden durch den Ersteller der GA-Anlage (in aller Regel in Zusammenarbeit mit den IT-Verantwortlichen des Kunden/Gebäudebetreibers/Bauherrn) projektiert und realisiert. Er legt fest, ob die GA oder wenigstens die Automationsebene auf einem separaten, für die GA dedizierten Netzwerk betrieben wird, ob eine Internetanbindung für die Fernkommunikation benötigt wird, wie das Netzwerk segmentiert wird, welche Sicherungsmassnahmen wie Firewalls, VPNs etc. für die Zugangspunkte eingesetzt werden, wie allfällige WLANs abgesichert werden. Die Bauherren und Fachplaner geben dabei die Funktionsanforderungen und den Kostenrahmen dafür vor.

Die Anstrengungen für die IT-Sicherheit erstrecken sich über den gesamten Werde-gang einer Anlage. Sie beginnen wie beschrieben beim Hersteller der eingesetzten Geräte und Programme und werden weitergeführt bei der Projektierung, Realisierung und Inbetriebsetzung der Anlage. Aber auch danach noch, in der Betriebsphase, sind für eine nachhaltige IT-Sicherheit dauerhafte Anstrengungen durch die Wartung und durch den Betreiber/Benutzer unerlässlich.

Eine Erfüllung des geforderten Sicherheitsstandards kann nur erreicht werden, wenn alle beteiligten Instanzen ihren Beitrag dazu leisten.



Abb. 2: Massnahmen nach Zuständigkeitsebene

3.1 Elemente auf Herstellerebene

Betroffen sind Geräte mit einem (eingebetteten) Betriebssystem (Automationsstationen, Netzwerkgeräte, intelligente Sensoren, Smart Actuators), sowie die Software für die Management-Ebene (SCADA/MBE/BEMS-Software, Energieanalyse- und Energiemanagementsoftware)..

Als Hersteller hat SAUTER sich bei der Entwicklung von modulo 6 an der IEC 62443-3-3 angelehnt, um Massnahmen und Lösungen zur Cyber Security zu integrieren. Hierzu gilt das Dokument [1] als Leitfaden. Einige der Massnahmen, sind:

Identifizierung / Authentifizierung, Zugangsberechtigung

Sowohl auf modulo 6 wie auf SAUTER Vision Center sind die Webserver-Benutzerkonten mit unterschiedlichen Berechtigungsebenen und Passwortanforderungen konfigurierbar. Das Ändern des Standardpassworts ist bei modulo 6-Stationen obligatorisch.

Nutzungskontrolle

Dank der integrierten Access Control Liste können Zugriffe von andern Teilnehmern im Netzwerk sowohl explizit erlaubt (Whitelist), als auch explizit verhindert (Blacklist) werden.

Protokollierung

Der in den modulo 6 Stationen eingebettete Webserver speichert alle Benutzeraktionen in Form eines Audit Trails. Somit sind alle Benutzereingriffe rückverfolgbar. Ähnlich bei SAUTER Vision Center, wo sogar höhere Anforderungen gemäss FDA Cfr 21 Part 11 unterstützt werden.

Integritätsprüfung

Mit der Building Data Integrity Solution ist eine Lösung vorhanden, welche periodisch die Integrität der Dateien auf allen Stationen einer Anlage prüft.. Diese Lösung nutzt eine Blockchain-Technologie, Verschlüsselung (TLS) und 2-Faktoren-Authentifizierung als Standard-Funktionen.

Rechtzeitige Reaktion auf Ereignisse

Bei Integritätsbruch wird ein Alarm ausgelöst und bei Bedarf die Ur-Konfiguration erneut auf die betroffenen Stationen geladen.

Verschlüsselung

Die Nutzung von TLS ist in modulo 6 Standard. Alle Protokolle die das unterstützen, nutzen dies, wie z. B. der Webserver mit https. Weiter wird BACnet/SC integriert, so dass BACnet nicht mehr in Klartext kommuniziert, sondern nur noch mit vorregistrierten Stationen, die auch BACnet/SC unterstützen. BACnet/SC nutzt TLS und ist nur in verschlüsselter Form verfügbar.

Netzwerktrennung: 2 Netzwerk-Schnittstellen

Das erlaubt z. B. die Automationsstation am Corporate-IT-Netzwerk anzuschliessen, um Zugang auf den Webserver zu ermöglichen, sowie den Zugang auf Cloud-Services wie Meteoserver oder E-Mail-Server für die Automationsstation. Gleichzeitig kommuniziert die Automationsstation mit BACnet/IP über ein physikalisch getrenntes Netzwerk mit der Gebäudeautomation. Somit wird der Datenfluss wirkungsvoll begrenzt.

Backup/Restore

Diese primäre Funktionalität wird von der kompletten Tool-Chain unterstützt. Sowohl die Konfiguration, wie auch das Regelungsprogramm werden mit dieser Funktion wiederherstellbar gesichert. Mit Building Data Integrity kann diese Wiederherstellung sogar automatisch durchgeführt werden, sobald eine unzulässige Integritätsverletzung / Datenänderung detektiert wird.

Verfügbarkeit

Die interne Architektur von modulo 6-Stationen priorisiert die Regelungsfunktionen gegenüber alle anderen Tasks, so dass bei Überlastung der Schnittstellen (z. B. bei Fehlkonfiguration im BACnet Netzwerk, oder DoS-Angriff auf den Webserver) die betroffene Schnittstelle blockiert wird und die Regelung weiterhin vollumfänglich autonom ausgeführt wird..

3.2 Zugangsrechte-System / Passwortschutz

Es ist klar, dass bei allen Geräten und Softwareprodukten, die über Benutzerzugänge (Webserver, Konfigurationszugänge etc.) verfügen, diese mit einem konfigurierbaren Zugangsrechtssystem mit Passwortschutz ausgestattet sein müssen.

Auch die Datenschnittstellen, welche die Geräte/Softwareprodukte für die Kommunikation mit ihren Datenquellen verwenden, sollten mit einer angemessen verifizierten Identifikation vor unerlaubtem Zugriff geschützt sein. (z.B. die Datenquellen der Energieanalyse- und Energiemanagementsoftware)

Die Sicherheit kann zusätzlich stark verbessert werden, wenn der Passwortschutz erweiterte Funktionen, wie Anforderungen an die Passwortkomplexität, ein Autologout bei Nichtbenutzung, eine zeitliche Sperrung nach einer vordefinierten Anzahl erfolgloser Login-Versuche, oder eine periodische PW-Ablaufzeit unterstützt.

Weiterhin soll bei der Bestimmung der Zugangsrechte der Zugang auf das Nötigste beschränkt werden - also nur soviel anzeigen, wie notwendig (need-to-know), nur soviel Anbieten wie notwendig (least functionality).

Vordefinierte mindest-PW-Anforderungen

Die Passwortkomplexität, das Autologout, die zeitliche Sperrung und die periodische PW-Ablaufzeit sind wichtige Features für einen guten Schutz.

Der Hersteller sollte in seinen Produkten solche Funktionalitäten bereitstellen, so dass diese bei der Inbetriebnahme dem Sicherheitsniveau der Anlage entsprechend festgelegt werden können. Programmiert der Hersteller die Mindestanforderungen fest in seine Produkte ein und diese können später nicht mehr dem Sicherheitsniveau der Anlage angepasst werden, sind sie womöglich oft nervend zu hoch.

Sinnvoll ist jedoch, wenn ab Fabrik fest vorgegeben ist, dass wenigstens der vom Hersteller eingerichtete Admin-Benutzer mit seinem Standard-PW nach

der Inbetriebnahme, d.h. nach einer vordefinierten Betriebszeit oder nach einem vordefinierten Kriterium geändert werden kann, oder besser, zwingend geändert werden muss. Viele der medial gross aufgemachten Hacker-Fälle basieren auf genau diesem Mangel. Das Standard-PW wurde nach der Inbetriebsetzung nicht geändert und im Internet finden sich Listen mit diesen Passwörtern diverser Hersteller.

Verschlüsselte Kommunikation https, SSH

Für die Absicherung der Kommunikation müssen die Produkte in der Lage sein, für ihren Webserver und ihre Konfigurationsschnittstellen eine TLS-gesicherte Kommunikation (https, SSH) zu verwenden. Nebst der Verschlüsselung der Kommunikation werden damit auch die Kommunikationsteilnehmer zuverlässig identifiziert. (Durch Zertifikate, wenn mit einer Public Key Infrastructure, PKI betrieben)

Interne Firewalls (Ports)

Alle netzwerkfähigen Geräte eines Systems (i.d.R. mit Linux-Betriebssystem) sollten mit einer werkseitig installierten und vorkonfigurierten Firewall gesichert sein. Damit sind alle Ports, die nicht für den regulären Betrieb verwendet werden, unerreichbar. Auch bei den Softwareprodukten sollten nicht benutzte / nicht benötigte Ports im Auslieferungszustand, d.h. nach einer Standardinstallation, nicht erreichbar sein. Für eine optimale Anpassung an das Sicherheitskonzept der Infrastruktur sollten die benutzten Portnummern für die verschiedenen Dienste frei konfigurierbar bleiben. Auch empfehlenswert ist, dass gegen einen Port Scan nur die effektiv verfügbaren Ports eine positive Antwort geben, und alle anderen gar keine.

Gehärtete Geräte / SW

Alle betroffenen Geräte und Softwareprodukte sollten ab Werk vorgehärtet ausgeliefert werden. Das heisst, alle nicht benötigten Dienste und Zugänge sollten nicht installiert resp. ab Werk deaktiviert sein. Standard IT Funktionalitäten wie Telnet (Port 23) oder FTP (Port 20) bieten Hackern zusätzliche und hinlänglich bekannte Einfallstore in die Gebäudeautomationshardware. Hier sind auch verschlüsselte Varianten zu bevorzugen (SSH, FTPS).

Audit-Trail-Funktionen (mit Signatur)

Für die nachträgliche Analyse eines echten oder auch eines vermeintlichen Angriffs (Fehlbedienungen, Spielereien), sollten möglichst alle Systeme Audit-Trail-Funktionen (die Aufzeichnungen von Benutzeraktivitäten) unterstützen. Diese helfen nicht nur herauszufinden, wer der Angreifer/Verursacher war, sondern auch wo allfällige Schäden oder Folgen liegen und korrigiert werden müssen.

Für die zuverlässige Nachverfolgbarkeit seriöser Angriffe sollten diese Aufzeichnungen mit einer Signatur gesichert werden können, damit sie nicht

vorsätzlich vom raffinierten Angreifer selbst oder unabsichtlich, von unvorsichtigen Untersuchungspersonen verändert werden können.

Security-relevante Updates-/Upgrades

Wie jede Technologie in der IT entwickeln sich auch die Angriffstechniken für IT-Einrichtungen permanent und mit hohem Tempo weiter. Alle betroffenen Produkte müssen entsprechend periodisch gepflegt und aktualisiert werden. Der Hersteller von GA-Produkten muss dazu für seine Produkte die Sicherheitsrelevanten Updates-/Upgrades und die entsprechenden Verteilkanäle bereitstellen.

Elemente auf Projektierungsebene

Bei der Projektierung der Gebäudeautomation werden (unter vielem anderem) die IT-Infrastruktur und ihre Sicherheitselemente festgelegt. Es geht um die Definition der Topologie (der Netzwerke und -Segmente), um die Schutzmassnahmen an den Zugangspunkten und um die Festlegung der Sicherungsmassnahmen, die auf den PC der Management-Ebene installiert werden müssen, etc...

Nicht vergessen werden sollte auch schon zu diesem Zeitpunkt die Vorplanung von Massnahmen, für den Eintretens-Fall von Störungen (infolge eines Angriffs).

Für diese Phase sind die Bauherren und Fachplaner stark mitbestimmend. In ihren Aus-schreibungen und Leistungsverzeichnissen werden die technischen Anforderungen nachgefragt und der Kostenrahmen gesprochen, welcher schlussendlich die Sicherheitsmassnahmen erst ermöglicht.

Risiko-/Schwachstellenanalyse

Eine Risikoanalyse bildet die Basis für die Projektierung der angemessenen Abwehrelemente. Weil das Risiko nicht für jeden Gebäudetyp und nicht für jede GA dasselbe ist, ist eine projektspezifische Risikoanalyse unerlässlich. Sie bestimmt das Ausmass der Sicherheitsvorkehrungen. Die Einflussfaktoren sind die Sensibilität des Gebäudes und der Umfang der GA-Funktionen (HLK, Licht, (Feuer-)Türen, Zutrittssysteme...).

Phys. separates GA-IP-Netzwerk / Segmentierung

Da moderne GA-Systeme den IP-Standard (OSI-Layer 3) als Basis für praktisch ihre gesamte Kommunikation verwenden, ist es natürlich verlockend, aus Kostengründen die in der Regel ohnehin bestehende IP-Netzwerkinfrastruktur eines Gebäudes mitzubenutzen. Es dürfte aber klar sein, dass dies Punkto IT-Sicherheit für die GA nicht die beste Lösung darstellt. Abgesehen von allfälligen Performance- und Verfügbarkeitsaspekten kann der Schutz der Netzwerke nicht optimal auf die Erfordernisse der GA angepasst werden, weil auch Anforderungen anderer Anwendungen zu berücksichtigen sind. Weiterhin bringt eine solche gemeinsame Nutzung der

Netzwerkinfrastruktur viele Nutzer und möglicherweise zusätzliche Zugänge und damit entsprechende Risiken direkt ins GA-Netzwerk.

Mit Firewalls gesicherte Netzwerke/Segmente

Der Schutz aller Netzwerkzugänge durch Firewalls ist eine der wichtigsten und wirksamsten Massnahmen zur Erhöhung der IT-Sicherheit gegen unberechtigte Zugriffe. Die Firewall überprüft jedes eintreffende Netzwerkpaket vor dessen Weiterleitung, basierend auf Absender-/Zieladresse und den genutzten Diensten.

Firewalls mit zusätzlichen Kontrollfunktionen verbessern die Sicherheit weiter. Solche FW überprüfen nicht nur die Adressierungsinformationen der eintreffenden Pakete, sondern auch weitere Kriterien. Z.B. analysieren sie den Paketinhalt (Deep Packet Inspection, DPI), bevor sie ihnen Zugang zum Netzwerk gewähren.

Es gibt Firewalls, die auch den ausgehenden Datenverkehr filtern. Damit stehen Schad-programmen, die von den betroffenen Maschinen nicht erkannt werden, zusätzliche Hürden für ihre Kommunikation im Weg.

Mit einer feineren Segmentierung der betroffenen Netzwerke kann deren Sicherheit weiter erhöht werden. Diese Unterteilung eines LAN erlaubt es, jedes einzelne der dadurch entstandenen kleineren Teilnetzwerke an seinen Grenzen wiederum durch Firewalls zu schützen. Damit kann die schädliche Wirkung von infizierten Maschinen innerhalb des LAN besser limitiert werden.

Firewalls sind heute oft zusammen mit dem Router im selben Gerät integriert. Auch werden die Funktionen von Firewalls zusehends von immer intelligenteren Switches abgedeckt. Alle drei Funktionalitäten wachsen in hardwaremässig immer leistungsfähigeren Geräten mehr und mehr zusammen.

VPNs für abgesetzte Stationen/Inseln

Abgesetzte Stationen oder abgesetzte Inseln über ein VPN (Virtual-Private Network) mit dem GA-System zu verbinden, erhöht die Gesamtsicherheit sehr substantiell.

Das VPN baut einen verschlüsselten Kanal zwischen der Remotestation/-Insel und dem anlageinternen LAN/Segment auf. Wie der Name sagt, wird damit die Remotestation/Insel virtuell in dieses LAN/Segment integriert. Die Kommunikation wird verschlüsselt und die Identität jedes VPN-Teilnehmers wird durch ein Passwort sichergestellt. Wird für die Verschlüsselung (TLS) ein Zertifikat (ab Public Key Infrastructure) für die Identifizierung verwendet, wird es für Unbefugte praktisch unmöglich, einen solchen Zugang abzuhören oder ihn für ihre Zwecke zu missbrauchen.

Abgesetzte Stationen mit VPN zu sichern lohnt sich nicht nur für weit entfernte Stationen (im WAN/Internet), sondern bei grösseren Netzwerken auch für Stationen in anderen Segmenten.

Switches mit Security-Funktionen

Vor allem wenn trotz der weiter oben erwähnten Einwände eine bestehende Netzwerkinfrastruktur durch die GA und andere Nutzer gemeinsam genutzt werden soll, hilft der Einsatz von Switches mit integrierten Security-Funktionen. Diese können die Sicherheit der an diesem gemeinsam genutzten Netz angeschlossenen GA-Komponenten stark verbessern, indem sie den Datenverkehr zu jedem einzelnen Teilnehmer filtern. Der Switch stellt sicher, dass jeder Teilnehmer ausschliesslich die Datenpakete erhält, die effektiv auch für ihn bestimmt sind.

Höher entwickelte Switches sind weiter in der Lage, ausgewählte Teilnehmer eines Netzes (z.B. die GA-Teilnehmer) zu einem VLAN zusammenzufassen. Damit kommunizieren diese innerhalb ihres eigenen, virtuellen Netzwerks und sind für die anderen Netzwerkteilnehmer nur sicht- und erreichbar, wenn dies mittels eines Routers/Firewall explizit ermöglicht wird.

Zum Teil können solche Switches auch manuell mit White-Lists/Black-Lists konfiguriert werden. In diesen Listen wird bei der Inbetriebnahme fix festgelegt, welche Geräte (auf Basis MAC-Adresse) an welches Port angeschlossen werden können und welche nicht. Dies verunmöglicht den Anschluss von fremden Rechnern ans GA-Netzwerk.

WLAN-Zugänge WPA2 (-Enterprise)

Sind (mobile) Geräte vorgesehen, die über WLAN (Wireless LAN) mit der Anlage verbunden werden sollen, so weist nur ein WLAN (WLAN-Router), welches den WPA2(-Enterprise)-Standard unterstützt ein zeitgemässes und gutes Sicherheitsniveau auf.

Beim WPA2 Sicherheitsstandard wird die Kommunikation basierend auf dem Advanced Encryption Standard (AES) verschlüsselt.

Im Gegensatz zu WPA2 ohne „Enterprise“, wo für die Identifizierung ein (dasselbe) Passwort für alle (Preshared Key) verwendet wird, unterstützt die Variante „Enterprise“ individuelle Passwörter, entweder von Benutzerkonten (LDAP/Active Directory, RADIUS), oder über Zertifikate (ab Public Key Infrastructure).

WPA2 und v.a. WPA2-Enterprise gilt bei Verwendung von ausreichend langen und komplexen Passwörtern und deaktiviertem WPS als heutiger Sicht als sehr schwierig bis nahezu unknackbar.

Malware-Schutz & Aktualisierung für PC

Nebst dem Netzwerkschutz, muss während der Projektierungsphase auch festgelegt werden, welcher Malwareschutz auf den beteiligten Management-PC installiert werden soll. Damit dieser dauerhaft wirksam bleibt, muss auch ein praktikables Aktualisierungskonzept mitdefiniert werden.

Der Malwareschutz verhindert die Wirkung von bekannten Computerviren, Computerwürmern, Trojanischen Pferden etc. und beseitigt diese, wenn

möglich. Da nur bekannte Schadsoftware erkannt werden kann, ist es wichtig, dass eine dauernde Aktualisierung sichergestellt ist.

Back-up Konzept inkl. Recovery-Anweisungen

Eine fachgerechte Back-up Einrichtung ist für ein GA-System ohnehin eine Selbstverständlichkeit.

Es muss damit gerechnet werden, dass die GA nach einem Angriff nicht mehr funktionsfähig ist, mit entsprechenden Folgen bei der Nutzbarkeit des betroffenen Gebäudes. Damit wird die Wiederherstellung der Funktion womöglich unter sehr grossem Zeitdruck zu erfolgen haben. Eine von Beginn weg existierende und klar definierte Vorgehensweise mit einer (getesteten und geübten, siehe weiter unten) Schritt für Schritt Recovery-Anweisung ist in diesem Fall eine unschätzbare Hilfe.

Da die Back-up Dateien in der Regel auch Kopien von hochsensiblen Daten enthalten werden, ist es wichtig schon bei der Projektierung mit einzuplanen, wo diese zuverlässig geschützt aufbewahrt werden können. Besondere Beachtung verdienen dabei z.B. Inhalte mit Systemkonfigurationsinformationen und die Daten der Benutzerverwaltung, die für einen versierten Hacker ausserordentlich nützlich sind!

Physische Anlage/Schaltschranksicherung

Sowohl für die Verhinderung eines echten Angriffs mit böser Absicht, wie auch von leichtsinnigen Zugriffen durch unbefugte Personen darf in diesem Zusammenhang natürlich die physische Sicherung der Anlage, der Schaltschränke und Kommunikationseinrichtungen nicht unerwähnt bleiben.

Im Kontext der IT-Sicherheit ist v.a. die Absicherung der physikalischen Zugangspunkte an den Geräten, Schaltschränken und den Kommunikationseinrichtungen zu erwähnen. Freie, wie auch belegte Ethernet-, USB-, Konfigurationssteckdosen an PCs, ASn, Routern etc. dürfen keinesfalls zugänglich sein.

Notbetriebmöglichkeiten (ohne GA)

Falls ein Angriff mit Folgen auf die Funktionsfähigkeit der GA eintreten sollte, können Notbedieneinrichtungen an den AS und den Anlagen selbst eine enorm wichtige und vieles rettende Bedeutung erhalten.

Dasselbe kann auch für Hardwareverriegelungen bei den technischen Installationen selbst gesagt werden (z.B. Ventilator darf nicht laufen, wenn Klappe ganz zu, etc.).

Elemente auf Inbetriebsetzungsebene

Während der Inbetriebsetzungsphase müssen die Vorgaben der Projektierung betreffend IT-Sicherheit umgesetzt und komplettiert werden. Alle sicherheitsrelevanten Parameter (Berechtigungen, Passwortvorgaben, Ports, etc. etc.) müssen eingestellt und soweit dies möglich ist, die Schutzmassnahmen auf ihr Funktionieren getestet werden. Für den

nachfolgenden Betrieb und die Wartungen müssen Updateabonnemente eingerichtet und die zukünftigen Benutzer geschult werden.

Angepasste (minimalisierte) Berechtigungen

Bei der Inbetriebsetzung werden für alle betroffenen Geräte/PC und Systeme die Benutzer/Benutzergruppen angelegt und ihre Rechte definiert. Je besser und exakter dabei die Rechte an die Aufgaben der Benutzer/Gruppen angepasst (heißt eingeschränkt/minimiert) werden, desto kleiner wird das Risiko. Das Risiko für gezielte Angriffe ebenso wie jenes für unbeabsichtigte Fehlbedienungen. Hier gilt grundsätzlich das „Need-to-know“ / "Least functionality" Prinzip, also nur Zugang freigeben, auf die Daten und Funktionen die dem Nutzer nötig sind und keine mehr.

Die Wichtigkeit dieser Anpassung bekommt zusätzliches Gewicht, wenn man an illegal beschaffte Log-In-Daten (Benutzername mit PW) oder an das Vorfinden von Geräten/PC mit eingeloggtem Benutzer denkt.

PW-Vorgaben/-Ablaufzeit, Autologout

Viele Geräte, Betriebssysteme und Programme bieten die Möglichkeit, diese Parameter ein-zustellen. Wie komplex muss ein Passwort aufgebaut sein? Welche Einschränkungen gibt man vor? Wie oft muss der Benutzer das Passwort wechseln? Nach wie viel Zeit ohne Benutzeraktivität wird er automatisch ausgeloggt? Die Risikoanalyse bestimmt, wie hoch die Anforderungen festgelegt werden sollten.

Es gilt dabei jedoch das Ganze und die Praxis zu sehen.

Benutzerfreundlichkeit konkurriert hier gegen Sicherheit und es ist zu bedenken, dass je höher die Anforderungen an die Passwörter, desto schwieriger wird es für die Benutzer, damit umzugehen. Je länger und je komplizierter der Aufbau, je öfter es geändert werden muss, je mehr verschiedene Pass-wörter sich der Benutzer zu merken hat, desto eher ist er genötigt, diese irgendwo zu notieren. Er verwendet ja auch in seinem Privatleben Passwörter. Solche die seine Familienmitglieder wissen müssen oder solche die sie nicht wissen dürfen. Jedes System hat seine eigenen Passwortregeln. Irgendwann wird es unmöglich und die Folge sind Passwortlisten auf dem Smartphone. Passwörter in mehr oder weniger sicheren Freeware-Passworttresoren, Passwörter unter der Tastatur etc. etc..

Nachhärtung Geräte/PC/Komponenten

Nach abgeschlossener Installation und Konfiguration aller relevanten Elemente verbessert die (Nach-) Härtung aller Geräte (Linux) und PC die Sicherheit weiter. Dies bedeutet, möglichst alle unbenutzten Dienste, Zugänge, Benutzerkonten, Prozesse und Programme zu entfernen oder zumindest zu deaktivieren. Nur die für den gewünschten Betrieb effektiv notwendigen Elemente sollten auf den Geräten verbleiben. Je schlanker das System, desto weniger nützliche Werkzeuge findet ein Angreifer, desto schwieriger wird es für ihn.

Betroffen sind v.a. die PCs. Bei den Geräten (ASn etc.) sollte schon der Hersteller so gut wie möglich vorgehärtet haben (nicht mit-kompiliert haben).

Audit Trails (mit Signatur) für Nachverfolgung

Im Eintretens-Fall einer Störung werden jederzeit verfügbare und aktive Logbücher (Audit Trails) enorm wichtig. Sie dienen einerseits der Überwachung, andererseits kann mit ihrer Hilfe im Fehlerfall auch die System- bzw. Datenwiederherstellung stark vereinfacht werden.

Die Logbücher müssen bei der Inbetriebsetzung möglicherweise aktiviert und konfiguriert werden. Sie sollten zumindest alle Benutzeraktionen, Änderungen an den Daten und natürlich alle Schalt- und Einstellaktionen aufzeichnen.

Sie lassen sich auch für Betriebssysteme in Datenbanken und Routern einrichten. Damit wird die Überwachung weiter verbessert.

Da man davon ausgehen muss, dass besonders qualifizierte Angreifer nach einem Angriff versuchen werden ihre Spuren aus den Audit Trails zu entfernen, kann es bei sensiblen Anlagen angezeigt sein, diese mit einer digitalen Signatur zu sichern. Die digitale Signatur schützt die Aufzeichnungen mit einem Signaturschlüssel und verhindert jede nachträgliche Änderung.

Bei der Konfiguration der Logbücher ist auch an deren Langzeitbehandlung zu denken. Wie wird verhindert, dass sie zu gross werden? Müssen sie periodisch gesichert werden? Wie lange müssen die Inhalte aufbewahrt werden?

Arbeitsvorschriften/Verhaltensanweisungen

Abschliessende und getestete Arbeitsvorschriften/Verhaltensanweisungen (Standard Operating Procedure, SOP) betreffend IT-Sicherheit sollten ab Beginn des Anlagebetriebs auf zwei Ebenen vorhanden sein: Einerseits solche für den Normalbetrieb, welche mithelfen sicher zu stellen, dass alle Sicherheitselemente dauerhaft funktionsfähig und auf dem neuesten Stand gehalten werden. Andererseits solche für den Fall eines Angriffs/Störfalls mit den Abläufen/Informationen für die Aufklärung, Schadensbegrenzung und -bewältigung.

Die Arbeitsvorschriften/Verhaltensanweisungen (SOP) für den Normalbetrieb bestehen z.B. aus Arbeitsabläufen, Checklisten und vorteilhafterweise aus Erinnerungsfunktionen eines Kalenders. Sie sorgen bei Einhaltung dafür, dass alle sicherheitsrelevanten Elemente gepflegt werden: Ist der Malwareschutz auf dem neuesten Stand? Sind alle sicherheitsrelevanten Updates der Programme und Betriebssysteme installiert? Welche Sicherheitsmassnahmen müssen bei neu installierten/hinzugefügten Elementen durchgeführt werden? Wurden die Backups ausgeführt, korrekt abgelegt und wie wird die Wiederherstellung regelmässig getestet? Hat die Überwachungsstelle ihre Kontrollfunktion wahrgenommen? Diese Arbeitsvorschriften/Verhaltensanweisungen sind ein enorm wichtiger

Puzzlestein innerhalb der gesamten Anstrengung zur Risikovermeidung bzw. Risikominimierung.

Im Eintretens-Fall eines Ereignisses mit Folgen auf die Funktionsfähigkeit der GA, muss da-mit gerechnet werden, dass diese unter Umständen teilweise oder vollständig funktionsunfähig wird. Dies kann im Extremfall massive Auswirkungen auf die Nutzbarkeit des Gebäudes haben. Die Wiederherstellung der Funktion der GA wird dann unter sehr grossem Zeitdruck zu erfolgen haben. Existierende, klar definierte und machbare Verhaltensanweisungen mit Schritt für Schritt Anweisungen etc. werden dann eine unschätzbare Hilfe sein. Nebst den Wiederherstellungshilfen können sie auch Informationen enthalten über die ein-zuhaltenden Meldewege, Rufnummern, Eskalationsstufen, Sofortmassnahmen etc...

Benutzerinformation/-schulung

Im täglichen Betrieb der GA kann die IT-Sicherheit nur optimal sein, wenn alle involvierten Elemente ihren korrekten Beitrag leisten. Hier fällt dem Faktor Mensch, d.h. nebst dem Wartungsverantwortlichen v.a. auch den Betreibern/Benutzern eine grosse Wichtigkeit zu.

Ist die Anlage mit allen Sicherheitseinrichtungen korrekt aufgesetzt, werden die involvierten Menschen wohl zum grössten potentiellen Risiko.

Fehlbedienung der Anlage selbst (Spielereien, Experimentierereien), Fehlbedienung der Sicherheitseinrichtungen, unangemessener Umgang mit Zugangs- oder anderen Daten, unvorsichtiger Umgang mit den Kommunikationseinrichtungen, Gutgläubigkeit (Mail, Phishing etc.), stellen die wohl grössten Gefahren dar.

Nebst der Schulung des technischen Wissens, welches für die korrekte Bedienung aller Sicherheitseinrichtungen der Anlage unerlässlich ist, ist es enorm wichtig, den Mitarbeitenden ein Bewusstsein für das potentielle Risiko zu vermitteln und sie für die möglichen Gefahren zu sensibilisieren.

Werden die IT-Sicherheitsthemen in einer spezifischen Schulung (unabhängig von den restlichen Themen) behandelt, erhalten sie mehr Gewicht. Gelegentliche Auffrischungen des Wissens helfen, das Thema auch nach längerer Zeit ohne Vorfälle dauerhaft hoch zu halten. Nicht zu vergessen sind Einweisungen für neue Mitarbeiter.

Ein eigener Schulungsblock verdient das Thema Verhalten und Wiederherstellung nach Schadensfall.

Elemente auf Wartungsebene

Die Angriffstechniken für IT-Einrichtungen werden laufend weiterentwickelt. Entsprechend auch die Abwehrtechnologien. Möglicherweise entwickelt sich auch die GA-Anlage.

Aufgabe der Wartung (betr. IT-Sicherheit) ist es, alle installierten Elemente der IT-Sicherheit periodisch zu pflegen, zu aktualisieren und wenn angebracht, die Anlage den neuesten Entwicklungen anzupassen.

Security-relevante Updates / Upgrades

Alle Geräte und Programme, insbesondere die PC, deren Malwareschutz, die Kommunikationseinrichtungen wie Router, VPN-Geräte etc. müssen regelmässig mit den verfügbaren Updates gepflegt werden. Nur so sind diese Schutzmechanismen den sich andauernd weiterentwickelnden Angriffstechniken gewachsen.

Unter Umständen machen hierbei technische Entwicklungen auch Upgrades auf modernere oder umfassendere Versionen nötig.

Security-relevante Systemanpassungen

Die installierte Hard- und Software von GA-Anlagen hat die Tendenz zu bedeutend längeren Lebenszyklen als die der kommerziellen IT.

Die Entwicklung in der IT-Bedrohung resp. IT-Sicherheitstechnik kann nötig werden, dass nebst der Pflege der bestehenden Sicherheitsmassnahmen auch grössere, umfassendere Systemanpassungen vorgenommen werden müssen.

Periodische Security-/Backup-Tests

Für die Sicherstellung eines hochstehenden Abwehryniveaus sollten die Sicherheitsmassnahmen in vordefinierten Wartungsintervallen überprüft und so weit wie möglich getestet werden.

Auch die Abläufe nach einem Angriff/Störfall sollten immer mal wieder geübt werden. Dies betrifft v.a. auch die Wiederherstellung von Back-ups. So manches Back-up hat sich im Ernstfall als nicht verwendbar erwiesen.

In regelmässigen Abständen sollten im Rahmen von Sicherheitsreviews auch die Anlagebetreiber/Benutzer auf die Einhaltung ihres (IT-) Sicherheitsverhaltens überprüft werden.

Elemente auf Benutzerebene

Wie mehrfach betont, kann das IT-Sicherheitsniveau einer GA-Anlage nur gut sein und bleiben, wenn über die gesamte Lebensdauer alle involvierten Stellen ihre sicherheitsrelevanten Aufgaben erfüllen. Damit sind insbesondere auch die Benutzer im alltäglichen Betrieb gemeint. Sie wären auch die ersten, denen allfällige Unregelmässigkeiten auffallen müssten.

Benutzername/PW-Good-Practices

Wie oben erwähnt, wird bereits beim Hersteller, spätestens bei der Inbetriebsetzung, die geforderte Passwortkomplexität festgelegt resp. dem anlagespezifischen Risiko angepasst.

Darüber hinaus sind jedoch auch die Benutzer gefordert, die Passwörter so zu wählen, dass sie möglichst nicht geknackt werden können. Dies bedeutet, dass diese auf keinen Fall Elemente aus naheliegenden Inhalten wie Namen,

Namen des Partners/der Kinder, Geburtsdatum etc. enthalten sollten. Es gibt Hacker (auch Spieler/Experimentierer) die Algorithmen schreiben, die die Passwörter mit solchen Elementen von Personendaten abgleichen, um sie zu knacken.

Allgemein ist es für die Passwortsicherheit vor allem die Länge (mehr als die Komplexität etc.) die es ausmacht. Sehr gut geeignet sind also auch Prosa-Sätze, soweit es sich nicht um berühmte Zitate etc. handelt. Sie haben den grossen Vorteil, dass man sie sich besser merken kann. (Z.B. „1 x Sauter immer Sauter“ oder „meine liebste ist die beste“)

Auch gehört es natürlich zu den PW-Good-Practices (gute Angewohnheiten) die Passwörter nicht irgendwo aufzuschreiben und nicht auszuleihen.

Back-up Handling/Überwachung

Automatisierte Back-up-Abläufe müssen auf ihre korrekte und vollständige Ausführung überwacht werden. Allenfalls müssen externe Medien gewechselt werden. Periodisch müssen sie auf ihre effektive Brauchbarkeit getestet werden (siehe weiter oben).

Da die Back-up-Dateien normalerweise auch Kopien von hochsensiblen Daten enthalten, müssen diese an einem zuverlässig geschützten Ort aufbewahrt werden. Besondere Beachtung verdienen dabei z.B. Dateien mit Systemkonfigurationsinformationen und die Daten der Benutzerverwaltung, die für einen versierten Hacker ausserordentlich nützlich sind. Auch Engineeringdokumente wie Systemtopologien, Sicherheitskonzepte etc., sind für einen An-greifer mit ernstesten Absichten sehr nützliche Informationen und müssen (inkl. all ihrer Kopien) entsprechend geschützt aufbewahrt werden.

Gefahrenbewusstsein/Wachsamkeit

Wie oben erwähnt, müssen die Bediener der GA in dedizierten Schulungen zum Thema IT-Sicherheit umfassend über die möglichen Gefahren ausgebildet werden. Es ist enorm wichtig, sie zu sensibilisieren und zu motivieren, wachsam zu sein. Anomalitäten und Auffälligkeiten müssen erkannt und ernst genommen werden.

Wie so oft stellt der Mensch ein Hauptrisiko dar. Mit Phishing, mit gefälschten Programm-aktualisierungen, selbst über Gespräche kann versucht werden, an sensible Daten, Systeminformationen, an Benutzernamen und Passwörter mit möglichst hohem Rechte-Niveau heranzukommen.

Prozesse und Audits

Verschiedene Organisationen sind in diesem Bereich aktiv. Beispielsweise ist der Standard IEC 62443 eine gute Referenz und sehr nah verwandt mit der ISO 27000-Reihe. In diesen Referenzen werden verschiedene Aspekte der Sicherheit betrachtet; von der Produktentwicklung, über den ganzen Lebenslauf der Produkte bis hin zur Abkündigung. Aber auch die Prozesse, der Produktentwicklung, der Produkteverwender, wie z.B.

Systemintegratoren und schliesslich die Endnutzer werden betrachtet. Cyber

Security betrifft alle, die mit den Produkten und Systemen in Kontakt kommen. Wichtig ist, eine klare Zielsetzung zu definieren und die Mittel zum Zweck einzusetzen. Die IT-Sicherheit ist ein Prozess der immer im Einsatz ist und muss in der Lage sein, sich an wiederkehrende und wechselnde Bedrohungen anzupassen.

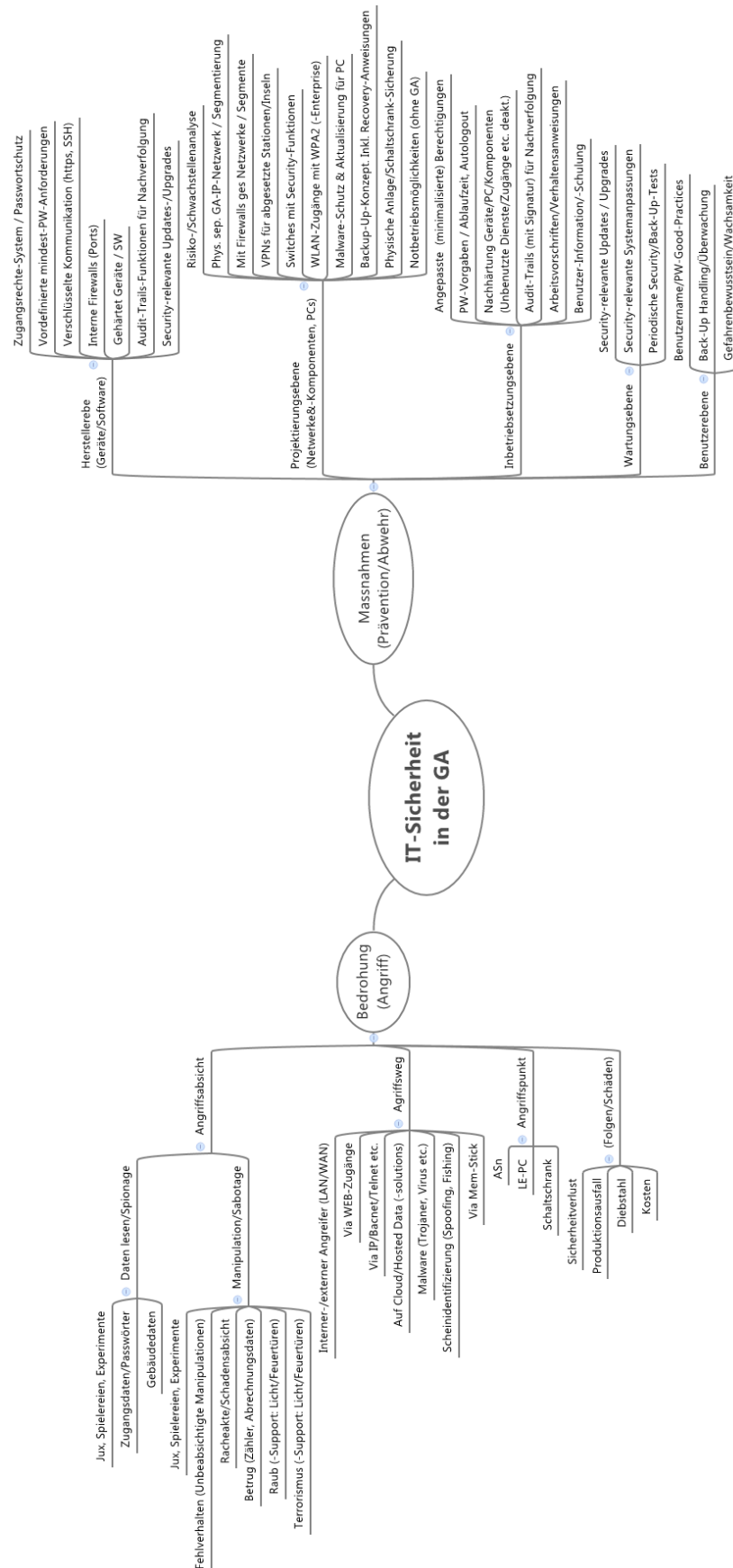


Abb. 3: Bedrohungen und Gegenmassnahmen der IT-Sicherheit für die GA

4 Schlussbemerkung

Die erreichbare, mögliche Spannweite für die IT-Sicherheit einer GA-Anlage ist enorm. Zwischen nichts tun und dem Realisieren aller möglichen Massnahmen liegen Welten. Von «jeder durchschnittliche IT-Fachmann kann eindringen» bis zu «enormem Aufwand / kaum machbar, auch für einen Hacker-Experten mit ernsthaften Absichten», gibt es jede Abstufung. Jede natürlich mit ihrem entsprechenden Aufwand und den entsprechenden Kosten!

Die Einschätzung des individuellen Risikos eines jeden Projekts ist zentral. Auch hier ist die Spannweite enorm. Für viele Gebäude geht die Gefahr wohl kaum über spielerisches, technisches Interesse, Jux, Prübeleien hinaus. Ein sehr grosses, sehr ernsthaftes Risiko besteht sicherlich bei Gebäuden, wo etwas zu holen ist, oder für die es offensichtlich Feinde gibt, oder für wichtige, öffentliche Gebäude mit einer ausgeprägten Sensibilität.

Grundlegende, dem branchenüblichen Stand der Technik entsprechende Sicherheitsmassnahmen sind für alle Gebäude dringendst empfohlen. Sie helfen gegen die meisten Angriffe und auch sehr gut gegen die oben erwähnten Spielereien/ Prübeleien. Sie können auch helfen, Fehlmanipulationen zu verhindern, welche zusammen mit den nie auszuschliessenden Softwarefehlern die wohl nach wie vor häufigste Ursache für Störungen sind.

Der Faktor Mensch ist wie so oft ein sehr wichtiges Element: Bedienerzugänge mit dauerhaft eingeloggtem Benutzer, Passwörter unter der Tastatur, ausgeliehene Passwörter, nicht geänderte Werks-Administrator-Zugänge. Kurz, mangelnde Sorgfalt, mangelndes Risikobewusstsein, mangelnde Wachsamkeit! Dagegen helfen regelmässige periodische Informationen und spezifischen Schulungen.

Der Autor

Franklin Linder, El.Ing. FH ist technischer Redaktor im SAUTER Head Office in Basel. Er verfügt über eine 20 jährige Erfahrung in der Entwicklung, Anwendung und Vermarktung von Gebäudeautomation.

Firmenportrait

SAUTER sorgt weltweit als führender Lösungsanbieter für Gebäudeautomationstechnologie in "Green Buildings" für gute Klimaverhältnisse und Wohlbefinden in Lebensräumen mit Zukunft. SAUTER entwickelt, produziert und vertreibt als Spezialist Systeme für energieeffiziente Gesamtlösungen und sichert mit umfassenden Dienstleistungen den energieoptimierten Betrieb von Gebäuden. Die Produkte, Lösungen und Dienstleistungen ermöglichen hohe Energieeffizienz während des gesamten Gebäudelebenszyklus von der Planung über die Realisierung bis zum Betrieb in Büro- und Verwaltungsgebäuden, Forschungs- und Bildungsstätten, Krankenhäusern, Industrie- und Laborgebäuden, Flughäfen, Freizeitanlagen, Hotels sowie Data Centers. Mit

über 100-jähriger Erfahrung und erprobter Technologiekompetenz ist SAUTER ein ausgewiesener Systemintegrator, der für kontinuierliche Innovation und Schweizer Qualität bürgt. Ausgezeichnet für bestes Automationssystem und beste Dienstleistung/Energy Service sowie eu.bac und BTL Zertifizierung für Produkte verschafft SAUTER Nutzern wie Betreibern die Übersicht über Energieflüsse und -verbrauch und somit auch über die Kostenentwicklung.

5 Literatur- /Quellenverzeichnis

-
- | | |
|-----|---|
| [1] | VDMA, V. D.-u. (2021-02). VDMA 24774:2021-02. IT-Sicherheit in der Gebäudeautomation. VDMA, Verband Deutscher Maschinen- und Anlagenbau. |
| [2] | IEC International Electrotechnical Commission. (2013-08). Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (1.0 ed.). Geneva, Geneva, Switzerland: IEC, Geneva, Switzerland. |
| [3] | VDMA, Verband Deutscher Maschinen- und Anlagenbau. (2016). Security in Automation - Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau. Produkt- und Know-how-Schutz. Berlin: HiSolutions AG. Von https://industrialsecurity.vdma.org/documents/16227999/16499033/1492086887896_INS_NAM_2016_Industrial_Security_IEC62443.pdf/c2e80bdb-c820-42cb-b3cc-fedd68571e1e |
| [4] | ZVEI, Zentralverband Elektrotechnik- und Elektronikindustrie. (2017). Orientierungsleitfaden für Hersteller IEC 62443. Frankfurt am Main: ZVEI. Von ZVEI, Zentralverband Elektrotechnik- und Elektronikindustrie: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Orientierungsleitfaden_fuer_Hersteller_IEC_62443/Orientierungsleitfaden_fuer_Hersteller_IEC_62443.pdf abgerufen |
| [5] | Cybersecurity for modulo 6. An Overview. Implementing IEC 62443 for Building Automation.2019-11, 5 th Revision, Fr. SAUTER AG. https://extranet2.ch.sauter-bc.com/wp-content/uploads/sites/13/2020/01/1071060-26.pdf |
-

6 Abkürzungsverzeichnis

Abkürzung	Begriff
z. B.	zum Beispiel
i.d.R.	In der Regel

7 Index

A

Abkürzungsverzeichnis	32
AES	
Advanced Encryption Standard	19
API	
Application Programming Interface	9
AS	
Automationsstationen.....	20

B

BACnet/IP	
BACnet over IP	14
BACnet/SC	
BACnet Secure Connect	14
BEMS	
Building Energy Management System	13
BYOD	
Bring Your Own Device	9

D

DPI	
Deep Packet Inspection	17

F

FTP	
File Transfer Protocol.....	16
FW	
Firewall.....	17

G

GA	
Gebäudeautomation.....	7, 9, 10, 11, 12, 13, 16, 17, 18, 19, 20, 22, 23, 24, 25, 29

H

HLK	
Heizung-Lüftung-Kälte	8, 9, 10, 17
https	
Hypertext transfer protocol secure	14, 15

I

IEC	
International Electrotechnical Commission	7, 8
International Electrotechnical Commission	7
IoT	
Internet of Things (Internet der Dinge)	7
IP	
Internet Protocol.....	17

IT	
Information Technology	7, 8, 9, 10, 12, 16, 17, 20, 22, 23, 24, 25, 29

K

KI	
Künstliche Intelligenz	9

L

LAN	
Local Area Network	17, 18, 19
LDAP	
Lightweight Directory Access Protocol	19
LoRaWAN	
Long Range Wide Area Network	9

M

MAC	
Media Access Control	18
MBE	
Management- und Bedienebene	13
MQTT	
Message Queuing Telemetry Transport	9

O

OPC	
Open Platform Communication (OLE for Process Control)	9
OSI	
Open Systems Interconnection (Model)	17

P

PC	
Personal Computer	7, 16, 19, 20, 21, 23
PKI	
Public Key Infrastructure	15
PW	
Password	15, 20, 24

R

RADIUS	
Remote Authentication Dial-In User Service	19

S

SCADA	
Supervisory Control and Data Acquisition	13
SOP	
Standard Operating Procedure	22
SPS	
Speicherprogrammierbare Steuerung	9
SSH	
Secure Shell	15

T

TLS	
Transport Layer Security	14, 15, 18

U

USB	
Universal Serial Bus	20

V

VLAN	
Virtual Local Area Netowrk	18
VPN	
Virtual Private Network	18, 23

W

WAN	
Wide Area Network	18
WiFi	
Wireless Fidelity	9
WLAN	
Wireless Local area Network	19
WPA2	
WiFi Protected Access	19
WPS	
WiFi Protected Setup	19