VDMA 24774

ICS 35.030; 35.240.67; 97.120

Ersatz für
VDMA 24774:2021-02

IT-Sicherheit in der Gebäudeautomation

IT Security for Building Automation and Control Systems

Gesamtumfang 19 Seiten

VDMA

Inhalt

Vorwort

Die Gebäudeautomation (GA) im IT-Umfeld wird zunehmend bedroht durch Schadensszenarien wie Sabotage, Spionage und das Aufspielen von Malware. Dies kann ungeschützt zu Datenmanipulation, Datenverlust und zum Ausfall der Gebäudeautomation mit Folgen wie Personenschäden oder Einschränkung des Geschäftsbetriebs (z.B. Produktionsausfall, Unbenutzbarkeit des Gebäudes) oder Vermögensschäden führen. Dieses VDMA-Einheitsblatt soll dabei helfen die Bedrohung durch Cyberangriffe zu erkennen, zu vermeiden oder deren Auswirkung zu minimieren.

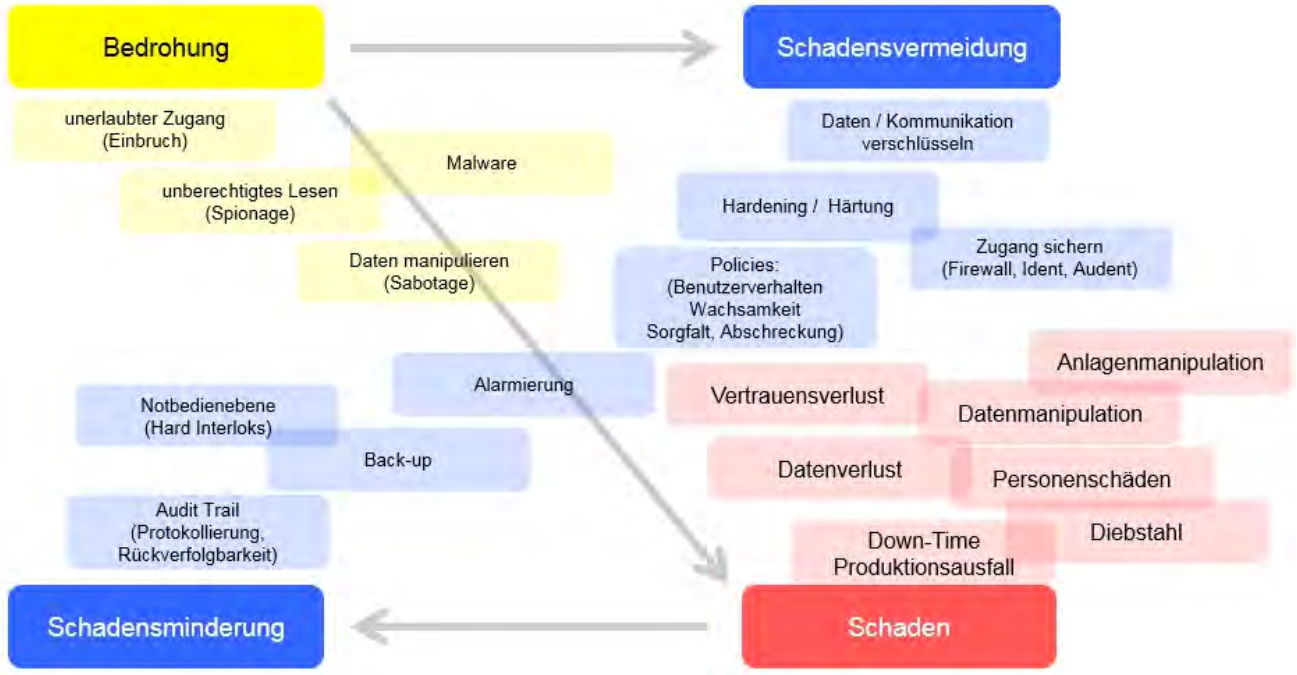

Bild 1 – Bedrohung - Gegenmaßnahmen in der Gebäudeautomation im IT-Umfeld

Die aktuelle Version dieses VDMA-Einheitsblattes wurde nach Veröffentlichung der Grundschutzbausteine Infrastruktur für Technisches Gebäudemanagement (INF.13) und Gebäudeautomation (INF.14) des bsi IT-Grundschutz-Kompendium überarbeitet, um die dort enthaltenen Anforderungen an die Gebäudeautomation abzubilden. Da sich das bsi IT-Grundschutz-Kompendium verpflichtend nur an Bundesbehörden und Betreiber kritischer Infrastrukturen richtet und alle Aspekte der IT-Sicherheit abdeckt, soll das VDMA-Einheitsblatt für alle an IT-Sicherheit der Gebäudeautomation interessierten und beteiligten Kreisen einen grundsätzlichen Einstieg in das Thema ermöglichen.

Das VDMA-Einheitsblatt soll Planer, Errichter und Betreiber dabei unterstützen, Maßnahmen für IT-Sicherheit von neuen oder schon errichteten GA-Systemen umzusetzen. Dies betrifft den gesamten Lebenszyklus inklusive Wartung, Service und Rückbau.

Änderungsvermerk

Gegenüber VDMA 24774:2021-02 wurden folgende Änderungen vorgenommen:

a) Überarbeitung zum Abgleich mit den Grundschutzbausteine Infrastruktur für Technisches Gebäudemanagement (INF.13) und Gebäudeautomation (INF.14)

Einleitung

Der Auslöser für die wachsende Bedrohung und die Aktualität des Themas IT-Sicherheit in der GA liegt in der technologischen Entwicklung.

In der gesamten Automatisierungstechnik wird seit längerer Zeit immer mehr Intelligenz in immer tiefere Ebenen verbaut. Speicherprogrammierbare Steuerungen (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.

In der Gebäudeautomation war die Entwicklung der letzten ca. 15 Jahre darüber hinaus geprägt von der Standardisierung der „offenen" Kommunikation (z.B. BACnet, KNX, LON). 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. Neuste Entwicklung in der GA gehen hin zu Cloudlösungen und IoT Technologien.

Durch die Nutzung allgemeiner IT-Standards für die Kommunikation wurde die Integration der GA 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 ermöglichen den Kunden und Betreibern der Gebäudeautomation Mehrwerte in Form von immer besseren Funktionalitäten, von unbegrenzten Kommunikationsmöglichkeiten und von völliger Wahlfreiheit bei Neu- und Erweiterungsprojekten.

Dadurch ergeben sich für die GA auch neue Dimensionen der Bedrohung, wie sie aus dem IT-Bereich bekannt sind.

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 Bedrohung. 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 Bedrohung 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. GA-Systeme steuern und regeln u. a. kritische Infrastrukturen, wodurch bei einem Cyberangriff größere wirtschaftliche Schäden oder Personenschäden entstehen können.

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

Um einen Basisschutz zu gewährleisten, müssen grundsätzliche Maßnahmen in allen Anlagen vorgesehen werden. Die IT-Grundschutz-Webseiten des Bundesamtes für Sicherheit in der Informationstechnik – BSI (www.bsi.de) geben hierzu Hilfsmittel an die Hand. Das BSI IT-Grundschutz-Kompendium bietet eine aktuelle Methode, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Das BSI stellt zahlreiche Werkzeuge zur Verfügung, um ein angemessenes Sicherheitsniveau zu erreichen.

Als Beispiel kann hier auch das kostenfreie Werkzeug des BSI Light and Right Security ICS (LARS ICS) genannt werden

(https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Tools/LarsICS/LarsICS_node.html),

mit dem der Einstieg in die Cyber-Sicherheit für kleine und mittlere Unternehmen aus dem Umfeld industrieller Steuerungsanlagen erleichtert wird. Es bietet eine fragengeleitete Selbsteinschätzung des aktuellen Stands der Cyber-Security und gibt Empfehlungen, welche Maßnahmen in welchen Bereichen als nächstes umgesetzt werden sollten.

Die Datenschutz-Grund-Verordnung – DSGVO zum Schutz personenbezogener Daten stellt weitere Anforderungen in Form von technischen und organisatorischen Maßnahmen für die GA. Dabei kann auch auf die Definitionen und Begriffe des BSI Grundschutzes zurückgegriffen werden.

Eine 100prozentige Sicherheit ist auch in der Gebäudeautomation selbst mit dem größten Aufwand nicht möglich. Ergänzend zu den Grundschutzkatalogen des BSI beschreibt dieses VDMA-Einheitsblatt die wichtigsten Maßnahmen zur Erhöhung der IT-Sicherheit in der Gebäudeautomation.

1 Anwendungsbereich

Dieses VDMA-Einheitsblatt behandelt die IT-Sicherheit in der Gebäudeautomation sowie den Schutz personenbezogener Daten und adressiert somit eine Basissicherheit für die Herstellung, die Planung und den Betrieb von GA-Systemen.

Den Aspekt der IT-Verfügbarkeit, 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.

Dieses VDMA-Einheitsblatt soll angewendet werden in Gebäudeautomationssystemen, die mittels Kommunikationsschnittstellen Daten austauschen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

DIN EN ISO 16484-5, *Systeme der Gebäudeautomation – Datenkommunikationsprotokoll (BACnet)*

DIN EN 13321-2, *Offene Datenkommunikation für die Gebäudeautomation und Gebäudemanagement – Elektrische Systemtechnik für Heim und Gebäude – Teil 2: KNXnet/IP-Kommunikation*

DIN EN 14908, *Firmenneutrale Datenkommunikation für die Gebäudeautomation und Gebäudemanagement – Gebäudedatennetzprotokoll (LON)*

DIN 32736:2000-08, Gebäudemanagement – Begriffe und Leistungen

VDMA 24186-4, *Leistungsprogramm für die Wartung von technischen Anlagen und Ausrüstungen in Gebäuden – Teil 4: MSR-Einrichtungen und Gebäudeautomationssysteme*

3 Begriffe

Für die Anwendung dieses VDMA-Einheitsblattes gelten die folgenden Begriffe.

3.1
Automationsstation
(auch Controller, Unterstation (veraltet))
Einrichtung zur Regelung und/oder Steuerung eines oder mehrerer physikalischer Werte, z. B. Temperatur, Feuchtigkeit, Druck.

3.2
BACnet
ein in DIN EN ISO 16484, Teil 5 genormtes Kommunikationsprotokoll für die Gebäudeautomation.

3.3
Cyberangriff (cyber attack)
global miteinander kommunizierende IT-Systeme (auch als Cyber-Raum bezeichnet) werden als primärer Angriffsweg benutzt oder werden selbst das Ziel eines Angriffs.

3.4
Deep Packet Inspection, DPI
vergleicht die Daten eines Protokoll-Paketes mit einer Datenbank von vordefinierten Angriffs-Signaturen (Zeichenketten); statistische oder historische Algorithmen können dabei die Überprüfung von statischen Mustern unterstützen

[Quelle: Dr. Thomas Porter, The Perils of Deep Packet Inspection, SecurityFocus.com, veröffentlicht 2005-01-11, aktualisiert 2010-10-19]

3.5
Feldgerät
physikalische Verbindung von der Eingabe-/Ausgabe-Schnittstelle einer Automationseinrichtung mit einem Anlagenteil für die notwendigen Informationen oder Aktionen, die Bedingungen, Zustände und Werte des Prozesses betreffend.

3.6
Firewall (Sicherheits-Gateway)
ein System aus soft- und hardware-technischen Komponenten, dass die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsrichtlinie ordnungsgemäß definierte Kommunikation gewährleistet.

3.7
FTP – File Transfer Protocol
ein im RFC 959 spezifiziertes Protokoll zur Übertragung von Dateien; es ist in der Anwendungsschicht (Schicht 7) des ISO/OSI-Schichtenmodells angesiedelt.

3.8
Gebäudeautomation – GA
Bezeichnung der Einrichtungen, Software und Dienstleistungen für automatische Steuerung und Regelung, Überwachung und Optimierung sowie für Bedienung und Management zum energieeffizienten, wirtschaftlichen und sicheren Betrieb der Technischen Gebäudeausrüstung.

3.9
HTTPS – Hyper Text Transfer Protocol Secure
ein im RFC 2818 spezifiziertes Web-Browser-Protokoll, das über TLS absichert ist.

3.10
IPv4 – Internet Protocol Version 4
ein im RFC 791 spezifiziertes Protokoll der Vermittlungsschicht (Network Layer) des ISO/OSI-Schichtenmodells.

3.11
IPv6 – Internet Protocol Version 6
ein im RFC 2460 spezifiziertes Protokoll der Vermittlungsschicht (Network Layer) des ISO/OSI-Schichtenmodells, das gegenüber der Version 4 einen wesentlich größeren Adressraum und einige weitere Verbesserungen enthält.

3.12
IT Sicherheit
definiert die Vertraulichkeit, Verfügbarkeit und Integrität von Daten.

3.13
IoT – Internet of Things
bezeichnet die Vernetzung physischer und virtueller Gegenstände miteinander, um sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

3.14
Cloud
die Bereitstellung von IT-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet. Technischer formuliert umschreibt das Cloud Computing den Ansatz, IT-Infrastrukturen über ein Rechnernetz zur Verfügung zu stellen, ohne dass diese auf dem lokalen Rechner installiert sein müssen.

3.15
KNX
ein in DIN EN 13321 spezifiziertes Kommunikationsprotokoll für Haus- und Gebäudeautomation.

3.16
LAN – Local Area Network, lokales Netz
ein privates Netz in einer Wohnung, einem Büro oder einer Fabrik; es verbindet Rechner, Automationsstationen, Bediengeräte, Drucker und andere netzwerkfähigen Komponenten.

3.17
LON
ein in DIN EN 14908 spezifiziertes Kommunikationsprotokoll für Haus- und Gebäudeautomation.

3.18
MAC-Adresse
die Hardware-Adresse einer Schnittstelle eines Gerätes in einem LAN.

3.19
Malware – schädliches Programm, Schadsoftware
Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte bzw. schädigende Funktionen auszuführen.

3.20
RFC – Request for Comments
eine Bezeichnung für technische Dokumente und Standards der Internet Community.

3.21
Router
Vermittler zwischen Netzwerken.

3.22
Schutzbedarfsfeststellung
Ziel der Schutzbedarfsfeststellung nach BSI IT-Grundschutz ist es zu klären, wie viel Schutz der betrachtete Informationsverbund und die ihm zugehörigen Objekte benötigen und damit die Auswahl angemessener Sicherheitsmaßnahmen für die einzelnen Objekte des betrachteten Informationsverbundes zu steuern.

3.23
Security-by-Design
Entwicklungsansatz, bei dem von Beginn des Entwicklungsprozesses an ein Sicherheitskonzept entworfen und umgesetzt wird.

3.24
SPS - Speicherprogrammierbare Steuerung
ein programmierbares Gerät, das zur Steuerung oder Regelung einer Maschine oder einer Anlage verwendet wird.

3.25
SSH – Secure Shell
ein Protokoll der Anwendungsschicht des ISO/OSI-Schichtenmodells mit umfangreichen Funktionen zur sicheren Authentisierung und zur Wahrung von Vertraulichkeit und Integrität, um sichere verschlüsselten Netzwerkverbindung zwischen netzwerkfähigen Komponenten herzustellen.

3.26
Switch
verbindet mehrere Netzwerk-Segmente miteinander.

3.27
Technisches Gebäudemanagement (TGM)
umfasst gemäß DIN 32736 alle Leistungen, die die technische Funktion und Verfügbarkeit eines Gebäudes erhalten. Zu diesen Leistungen gehören unter anderem:

– Betreiben,
– Dokumentieren,
– Energie- und Umweltmanagement,
– Informationsmanagement,
– Modernisieren,
– Sanieren,
– Umbauen,
– Verfolgen der technischen Gewährleistung.

3.28
TLS – Transport Layer Security
ist ein verschlüsseltes Datenübertragungsprotokoll der Transportschicht des ISO/OSI-Schichtenmodells; die zurzeit aktuelle Version 1.3 ist im RFC 8446 spezifiziert.

3.29
VLAN – Virtual Local Area Network
Abbildung einer logischen Netzstruktur innerhalb eines physikalischen Netzwerkes.

3.30
VPN – Virtuelles privates Netz
ein Netz, das physisch innerhalb eines anderen Netzes betrieben wird, jedoch logisch von diesem Netz getrennt ist. VPNs können unter Zuhilfenahme kryptographischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. Die sichere Authentisierung der Kommunikationspartner ist auch dann möglich, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

3.31
WAN – Wide Area Network, Weitverkehrsnetze
ein Netzwerk, das sich über einen sehr großen geografischen Bereich erstreckt.

3.32
WLAN – Wireless LAN (IEEE 802.11)
ein lokales Funk-basiertes Rechnernetz.

3.33
WPAN – Wireless Personal Area Network (IEEE 802.15.4)
ein lokales Funk-basiertes Netz, das von Kleingeräten genutzt wird.

3.34
WPA2-Enterprise-Standard – Wi-Fi Protected Access 2
Implementierung eines Sicherheitsstandards für WLANs, basierend auf dem Advanced Encryption Standard.

3.35
Digitales Zertifikat
ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.

4 Maßnahmen zur Prävention und Schadenabwehr

Der Lebenszyklus eines Gebäudes kann vereinfacht in 4 Phasen eingeteilt werden:

– Planung

– Realisierung

– Nutzung

– Rückbau

Ein gesamtheitliches IT-Sicherheitskonzept erfordert die Mitwirkung aller Beteiligten der 4 Phasen.

4.1 Elemente der IT-Sicherheit in der GA

Im Lebenszyklus einer GA-Anlage beginnen die Maßnahmen zur IT-Sicherheit auf der Ebene der einzelnen Geräte und Softwaren bereits beim Produkt-Hersteller. Er sollte schon ab Werk möglichst umfassende Sicherheitsmaßnahmen (gemäß des Security-by-Design Ansatzes in seine Produkte integrieren und dokumentieren, wie z.B. ein Zugriffsrechtesystem mit Authentisierungsmechanismus (z.B. Passwortschutz, die Unterstützung verschlüsselter Kommunikation, interne oder externe Firewalls usw).

Diese vorinstallierten Schutzmaßnahmen auf Ebene der Geräte/Software müssen nachfolgend bei der Anlagenerstellung und -inbetriebnahme weiter komplettiert und parametriert werden. Die Bauherren und Fachplaner geben dabei die Funktionsanforderungen für diese Maßnahmen vor.

Auf Maßnahmen auf Ebene der IT-Infrastruktur, d.h. der Netzwerke/Netzwerksegmente und deren Zugänge hat der GA-Produkt-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 Internet-anbindung für die Fernkommunikation benötigt wird, wie das Netzwerk segmentiert wird, welche Sicherheits-

maßnahmen wie Firewalls, VPNs etc. für die Zugangspunkte eingesetzt werden und wie WLANs abgesichert werden.

Auch in der Betriebsphase sind für eine nachhaltige IT-Sicherheit dauerhafte Maßnahmen durch Service und Wartung durch den Betreiber/Benutzer unerlässlich. Dazu gehört auch der Schutz personenbezogener Daten.

Beim Austausch von Komponenten und Rückbau einer GA sollte mit sensiblen Daten verantwortungsbewusst gemäß aktuellen Datenschutzbestimmungen (siehe DSGVO) umgegangen werden.

Eine Erfüllung des geforderten Sicherheitsstandards kann nur erreicht werden, wenn alle beteiligten Instanzen ihren Beitrag dazu leisten und die IT-Sicherheit aktiv gemanagt wird.

4.2 Risiko-/Schwachstellenanalyse

Eine Risikoanalyse bildet die Basis für die Projektierung der angemessenen Schutzmaßnahmen. Diese sollte von Bauherrn, Betreibern gemeinsam mit Fachplanern durchgeführt werden.

Weil das Risiko nicht für jeden Gebäudetyp und nicht für jede GA gleich ist, ist eine projektspezifische Schutzbedarfsfeststellung unerlässlich. Sie bestimmt das Ausmaß der Sicherheitsvorkehrungen. Der Schutzbedarf basiert auf der Sensibilität des Gebäudes und dem Umfang der GA-Funktionen (HLK, Licht, Brandschutz-Türen, Zutrittssysteme...).

Der Schutzbedarf eines Objekts orientiert sich an dem Ausmaß der Schäden, die entstehen können, wenn seine Funktionsweise beeinträchtigt ist. Da die Höhe eines Schadens häufig nicht genau bestimmt werden kann, sollte eine für den jeweiligen Anwendungszweck passende Anzahl von Kategorien definiert werden, anhand derer sich der Schutzbedarf unterscheidet.

Die IT-Grundschutz-Vorgehensweise des BSI empfiehlt drei Schutzbedarfskategorien:

– normal: Die Schadensauswirkungen sind begrenzt und überschaubar.

– hoch: Die Schadensauswirkungen können beträchtlich sein.

– sehr hoch: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Basierend auf dem Schutzbedarf ist zu bewerten, ob die Schutzmaßnahmen das Risiko auf ein tolerierbares Maß reduzieren. Durch die in diesem VDMA-Einheitsblatt beschriebenen Maßnahmen ist die Schutzbedarfskategorie „Normal“ abgedeckt. Für die Schutzkategorien „Hoch“ und „Sehr Hoch“ ist eine individuelle Betrachtung notwendig.

Bei der Risikobetrachtung sollte prinzipiell beachtet werden, dass Systeme von Dritten über den Missbrauch durch GA-Systeme angegriffen werden können (z.B. über BOT-Netze, infizierte USB-Sticks, …).

4.3 Hersteller-Ebene

Betroffen sind kommunikationsfähige Geräte, die an das Netzwerk angeschlossen sind (Automationsstationen (AS), Raumcontroller, Gateways, Netzwerkgeräte, evtl. intelligente Sensoren), sowie die Software für die Management-Ebene (SCADA-Software, Energieanalyse- und Energiemanagementsoftware).

4.3.1 Zugangsrechte-System/Passwortschutz

Alle Geräte und Softwareprodukte, die über Benutzerzugänge (Webserver, Konfigurationszugänge etc.) verfügen, müssen mit einem konfigurierbaren Zugangsrechtesystem mit Authentisierungsmechanismus (z.B. Passwortschutz) ausgestattet sein.

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). Bei der Kommunikation mit der Feldebene ist dies in vielen Fällen nicht gegeben, da gängige Protokolle dieses Maß an Sicherheit nicht vorsehen.

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

Der Hersteller sollte in seinen Produkten solche Funktionalitäten bereitstellen, so dass diese bei der Inbetriebnahme dem Sicherheitsniveau der Anlage entsprechend festgelegt werden können.

Es ist darauf hinzuweisen, dass Standard-Passwörter für voreingerichtete Benutzer nach der Inbetriebnahme, spätestens im Rahmen der Übergabe/Abnahme, d.h. nach einer vordefinierten Betriebszeit oder nach einem vordefinierten Kriterium, geändert werden. Komponenten, die keinen Zugangsschutz beinhalten, sollten dann abgeschaltet oder durch zusätzliche Maßnahmen geschützt werden. Alle voreingerichteten Benutzer müssen dokumentiert sein.

Der Zugangsschutz des Betriebssystems kann in den Produkten der GA integriert sein, um die Bedienung für den Nutzer zu vereinfachen unter Beibehaltung der für den Benutzer angegebenen Zugriffsrechten.

4.3.2 Verschlüsselte Kommunikation zum Nutzer (Webserver)

Für die Absicherung der Kommunikation sollten die Produkte in der Lage sein, für ihren Webserver und ihre Konfigurationsschnittstellen eine TLS -gesicherte Kommunikation nach Stand der Technik (siehe BSI Richtlinie TR-02102) zu verwenden.

4.3.3 Gehärtete Geräte und Software

Alle betroffenen Geräte und Softwareprodukte sollten ab Werk vorgehärtet ausgeliefert werden. Das heißt, alle nicht benötigten Dienste und Zugänge sollten nicht installiert bzw. ab Werk deaktiviert sein.

Alle verfügbaren Dienste und Zugänge sind zu dokumentieren. Die Sicherheitseigenschaften der verwendeten Netzwerk-Protokolle sollten dokumentiert sein.

Standard IT-Protokolle wie FTP bieten Hackern zusätzliche und hinlänglich bekannte Einfallstore in die Gebäudeautomation.

Tabelle 1 – Beispiel für Kommunikationsübersicht

Service	Port	Protocol	Description	Active (Y/N)
DNS	53	TCP	DNS proxy	
DNS	53	UDP	DNS proxy	
HTTP	80	TCP	Web server (config)	
HTTPS	443	TCP	Web server (config)	
DHCP	67	UDP	DHCP server	
DHCPv6	547	UDP	DHCPv6 server	
ICMPv6			ICMPv6 messages	
KNXnet/IP	3671			
BACnet/IP	47808			
…				

4.3.4 Audit-Trail-Funktionen

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

Für die zuverlässige Nachverfolgbarkeit eines Angriffs sollten diese Aufzeichnungen technisch gesichert werden können, damit sie nicht vorsätzlich vom Angreifer selbst oder unabsichtlich, von unvorsichtigen Untersuchungspersonen verändert werden können.

Die Vorgaben des DSGVO zum Schutz von personenbezogener Daten sind zu berücksichtigen.

4.3.5 Security-relevante Updates

Wie jede Technologie in der IT entwickeln sich auch die Angriffstechniken permanent und mit hohem Tempo weiter. Der Hersteller von GA-Produkten stellt für seine Produkte die sicherheitsrelevanten Abhilfemaßnahmen (z.B. Patches) im Rahmen von zu vereinbarenden Wartungsverträgen zur Verfügung. Der Hersteller arbeitet dafür bei Bedarf mit Zulieferern und Dienstleistern (z.B. Betriebssystemhersteller, Plattformbetreiber) zusammen.

4.4 Projektierungs-Ebene

Bei der Projektierung der Gebäudeautomation und bei der Übernahme von Bestandsgebäuden sind die Zustände zu bewerten und entsprechend in die Bearbeitung zu übernehmen. Dabei werden auch die IT-Infrastruktur und ihre grundlegenden Sicherheitselemente festgelegt.

Je nach Anlage/Gebäudetyp sind zu definieren und dokumentieren:

– Topologie der Netzwerke und -Segmente,

– Schutzmaßnahmen an Netzsegmentübergängen und den Zugangspunkten (LAN, WLAN, WAN, Physischer Zugang),

– Schutzmaßnahmen an Schnittstellen zu anderen Gewerken,

– Festlegung der Sicherheitsmaßnahmen. die auf den Rechnern und Servern der Management-Ebene installiert werden müssen,

– weitere Maßnahmen aus der Risiko-/Schwachstellenanalyse, sowie die Festlegung eines Inbetriebnahme- und Schnittstellenmanagements für die GA,

– Havarie Management (infolge eines Angriffs),

– Für die Kommunikation von GA-relevanten Komponenten die auf Ethernet und IP basiert, sollten sichere Protokolle eingesetzt werden, falls über nicht-vertrauenswürdige Netzsegmente kommuniziert wird (integritätssichere Datenübermittlung).

– Außerhalb vertrauenswürdiger Netzsegmente sollte die Kommunikation über Ethernet und IP zwischen GA-Systemen verschlüsselt erfolgen. Die Verschlüsselung sollte mit den jeweils aktuellen Verschlüsselungs-mechanismen durchgeführt werden.

– Für die GA sollte ein Identitäts- und Berechtigungsmanagement genutzt werden, das die Anforderungen der GA angemessen umsetzt.

– Abnahmetest der IT-Sicherheit

Für diese Phase sind die Bauherren und Fachplaner stark mitbestimmend. In ihren Ausschreibungen und Leistungsverzeichnissen werden die technischen Anforderungen vorgegeben, welche schlussendlich die Sicherheitsmaßnahmen erst ermöglichen. In dieser Phase sollten auch die Anforderungen, die sich aus einem TGM Konzept ergeben können, mit berücksichtigt werden.

4.4.1 Getrennte GA-IP-Netzwerke

Obwohl es sich anbietet bestehende IP-Netzwerkinfrastruktur eines Gebäudes mitzubenutzen, stellt dies für die IT-Sicherheit der GA eine Gefährdung dar. Abgesehen von Performance- und Verfügbarkeitsaspekten kann der Schutz der Netzwerke nicht optimal auf die Erfordernisse der GA angepasst werden, weil Anforderungen anderer Anwendungen zu berücksichtigen sind. Eine solche gemeinsame Nutzung der Netzwerkinfrastruktur bedeutet viele Nutzer und zusätzliche Zugänge und steigert damit die Risiken für das GA-Netzwerk.

Aus Gründen der IT-Sicherheit für die GA ist daher eine physikalische oder logische Trennung der GA-Netzwerke von anderen Netzwerken vorzusehen .

Jegliche Kommunikation zwischen GA-Systemen und sonstigen IT-Systemen muss kontrolliert und reglementiert werden. Hierfür müssen an allen Übergängen einer solchen Segmentierung entsprechende Komponenten mit Sicherheitsfunktionen, mindestens mit Firewall-Funktion, vorgesehen werden.

Bei erhöhtem Schutzbedarf sollten GA-Netze als physisch getrennte Zonen realisiert werden.

4.4.2 Mit Firewalls gesicherte Netzwerke/Segmente

Der Schutz aller Netzwerkzugänge durch Firewalls (FW) ist eine der wichtigsten und wirksamsten Maßnahmen zur Erhöhung der IT-Sicherheit gegen unberechtigte Zugriffe.

Segmente mit unterschiedlichem Schutzbedarf sollten ausreichend voneinander getrennt werden (z.B. GA zu IT-Netzwerk). 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 zu schützen. Damit kann die schädliche Wirkung von infizierten Systemen innerhalb des LAN besser limitiert werden.

Firewalls müssen im Rahmen der Projektierung und Inbetriebnahme an die entsprechende Gebäudeautomation konfiguriert werden.

4.4.3 Geschützte Kommunikation für abgesetzte Stationen, Inseln oder Fern-Service

Abgesetzte Stationen (außerhalb des LAN), Inseln oder Fern-Service müssen über eine geschützte Kommunikation (z.B. VPN (Virtual Private Network), https) mit dem GA-System verbunden werden.

Es empfiehlt sich zusätzlich den Zugriff solcher abgesetzter Stationen auf die GA z.B. durch den Einsatz entsprechender Firewall Regeln auf das Nötigste zu beschränken.

4.4.4 Switches/Router mit Sicherheits-Funktionen

Wenn eine Netzwerkinfrastruktur durch die GA und andere GA-fremde Nutzer gemeinsam genutzt werden soll, sollten Switches/Router mit integrierten Sicherheits-Funktionen genutzt werden. Diese verbessern die Sicherheit der an diesem gemeinsam genutzten Netz angeschlossenen GA-Komponenten, indem sie den Datenverkehr zu jedem einzelnen Teilnehmer filtern. Der Switch/Router stellt sicher, dass jeder Teilnehmer ausschließlich die Datenpakete erhält, die auch für ihn bestimmt sind.

Höher entwickelte Switches sind in der Lage, ausgewählte Teilnehmer eines Netzes (z.B. die GA-Teilnehmer) zu einem VLAN (Virtual Local Area Network) zusammenzufassen. Damit kommunizieren diese innerhalb ihres eigenen, virtuellen Netzwerks und sind für die anderen Netzwerkteilnehmer nur sicht- und erreichbar, wenn dies explizit im Netzwerkkonzept eingeplant und umgesetzt wird.

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

4.4.5 Funknetzwerke

Funknetzwerke sind aufgrund des einfachen physischen Zugangs gegenüber Angreifern besonders exponiert. Die einzusetzenden Technologien sind auf Basis einer Risikoabschätzung auszuwählen. Sind Geräte vorgesehen, die über WLAN (Wireless LAN) mit dem GA-Netzwerk verbunden werden, sollte ein WLAN (WLAN-Access-Point) mit aktueller Verschlüsselungstechnik (z.B. WPA3 -Standard) eingesetzt werden. Nach BSI Grundschutz sollen Kryptographische Verfahren unsicherer als WPA2 nicht mehr eingesetzt werden.

WPA3 gilt bei Verwendung von ausreichend langen und komplexen Passwörtern und deaktiviertem WPS aus heutiger Sicht als sicher.

Werden Kleingeräte, meist batteriebetrieben, in einem WPAN betrieben, sollte eine IP basierte Technologie verwendet werden, die den Einsatz von Standard IT Security Protokollen wie z.B. TLS unterstützt.

4.4.6 Daten- und Zeitsychronisierung

Ein GA-System sollte visualisieren, ob die angezeigten Informationen bezüglich Zeit, Ort, Wert, Zustand oder Ereignis auf planmäßig erhaltenen Informationen basieren. Informationen, die simulierte oder „eingefrorene“ Werte anzeigen, sollten abhängig vom Schutzbedarf der TGA-Anlagen erkennbar sein oder einen Alarm auslösen.

Alle in einem GA-System angebundenen Komponenten und TGA-Anlagen sollten eine synchrone Uhrzeit nutzen, um ein automatisiertes Messen, Steuern und Regeln zu gewährleisten. Auch GA-Systeme, die miteinander verbunden sind, sollten eine synchrone Uhrzeit nutzen. Erstreckt sich die GA über

Gebäudekomplexe oder Liegenschaften, sollte die Zeitsynchronisation mittels genormter Protokolle für alle Gebäude gewährleistet werden.

4.4.7 Schutz vor Schadsoftware

Neben dem Netzwerkschutz muss während der Projektierungsphase auch festgelegt werden, mit welchem Konzept der Schutz vor Schadsoftware auf den beteiligten Servern und Computern sichergestellt werden soll. Damit dieser dauerhaft wirksam bleibt, muss auch ein praktikables Aktualisierungskonzept mitdefiniert werden.

Wird auf einem System kein Virenschutzprogramm ausgeführt, beispielsweise aufgrund von knappen Ressourcen oder aufgrund von Echtzeitanforderungen, sollten geeignete alternative Schutzverfahren eingesetzt werden.

Der Schutz vor Schadsoftware 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.

Jedes externe System und jeder externe Datenträger sollte vor der Verbindung mit einem GA-System und vor der Datenübertragung auf Schadsoftware geprüft werden.

4.4.8 Back-up Konzept inkl. Recovery-Anweisungen

Sollte eine GA z.B. nach einem Angriff oder Ausfall nicht mehr funktionsfähig sein, ist mit entsprechenden Folgen bei der Nutzbarkeit des betroffenen Gebäudes zu rechnen. Eine existierende und klar definierte Vorgehensweise mit einer getesteten und geübten Schritt für Schritt Recovery-Anweisung ist erforderlich (siehe Abschnitt 4.5.5).

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 und geschützt aufbewahrt werden können. Besondere Beachtung verdienen dabei z.B. Inhalte mit Systemkonfigurationsinformationen, personenbezogene Daten und die Daten der Benutzerverwaltung.

4.4.9 Physische Anlage/Schaltschranksicherung

Sowohl für die Verhinderung eines Angriffs wie auch von Zugriffen durch unbefugte Personen sollte die physische Sicherung der Anlage, der Schaltschränke und Kommunikationseinrichtungen sichergestellt werden.

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

Insbesondere ist auf die Segmentierung von vernetzten Geräten im Raum (z.B. Bediengeräte der Raumautomation) zu achten, da diese je nach eingesetzter Technik eine Zugangsmöglichkeit zum GA Netzwerk darstellen kann.

Für frei zugängliche LAN- oder WLAN-Zugänge und kommunikative Systeme, die nicht physisch abgesichert werden können, sollte eine Netzzugangskontrolle gemäß IEEE 802.1X oder andere geeignete Sicherheitsmechanismen eingesetzt werden. Hiermit sollten unzureichend authentisierte und autorisierte Komponenten in getrennten Netzsegmenten positioniert werden. Frei zugängliche Schnittstellen für temporäre Wartungszwecke, wie beispielsweise USB-Ports an GA-Komponenten, sollten nur bei Bedarf aktiviert werden.

4.5 Inbetriebnahme-Ebene

Während der Inbetriebnahme-Phase müssen die Vorgaben der Projektierung betreffend der IT-Sicherheit umgesetzt und vervollständigt werden. Alle sicherheitsrelevanten Parameter (z.B. Berechtigungen, Passwortvorgaben, Ports) müssen eingestellt und, soweit dies möglich ist, die Schutzmaßnahmen auf ihre Funktionsfähigkeit überprüft werden. Bei der Inbetriebnahme müssen die aktuell freigegebenen Softwarekomponenten installiert werden. Für den nachfolgenden Betrieb und die Wartungen sollten Updateabonnements für z.B. Virenscanner eingerichtet und die zukünftigen Betreiber geschult werden.

Alle beteiligten Personen benötigen die für Ihre Tätigkeits- und Verantwortungsbereiche eine entsprechende Sensibilisierung. Hierzu muss kompetentes Personal in regelmäßigen Trainings zu Leitlinien und Vorgehensweisen unterwiesen werden. Dieses Vorgehen ist entsprechend nachhaltig zu dokumentieren. Dazu gehören unter anderen die vom Betreiber vorgegebenen Leitlinien und Prozesse z.B. zur Vornahme von Änderungen (Management of Change).

4.5.1 Anpassung der Berechtigungen

Bei der Inbetriebnahme müssen für alle betroffenen Geräte/PC und Systeme die Benutzer/Benutzergruppen angelegt und entsprechend ihrer Berechtigung definiert werden. Je besser und exakter dabei die Rechte an die Aufgaben der Benutzer/Gruppen angepasst (das heißt eingeschränkt/minimiert) werden, desto kleiner wird das Risiko für gezielte Angriffe und für Fehlbedienungen.

In dieser Phase müssen die ursprünglichen Standard- oder Default Zugänge durch projektspezifische Zugänge ersetzt, projektintern dokumentiert und dem Kunden übergeben werden.

4.5.2 Passwort-Vorgaben/-Ablaufzeit, Autologout

Viele Geräte, Betriebssysteme und Programme bieten die Möglichkeit, die Passwortregeln einzustellen z.B.:

– Komplexität

– Ablaufzeit

– Wiederholungen

– Autologout Zeit

Die Risiko-/Schwachstellenanalyse (siehe Abschnitt 4.2) bestimmt, wie hoch die Anforderungen sind, und bildet die Grundlage für die Inbetriebnahme.

Bei der Änderung der Passwörter ist darauf zu achten, dass die Beteiligten an Serviceprozessen (Entstörung, Rufbereitschaft, Wartungen etc.) über die Änderung informiert werden. Es muss sichergestellt werden, dass z.B. auch im Störungsfall der Wartungstechniker das System bedienen/um-parametrieren kann.

Die Einhaltung der Passwortregeln sollte durch organisatorische oder technische Maßnahmen sichergestellt werden.

4.5.3 Nachhärtung Geräte/PC/Komponenten

Am Ende der Inbetriebnahme sollten alle unbenutzten Dienste, physikalische Zugänge, Benutzerkonten, Prozesse und Programme entfernt oder deaktiviert werden; nur die für den Betrieb notwendigen Elemente sollten auf den Geräten verbleiben.

Alle aktiven Dienste und Zugänge sind zu dokumentieren. Die Sicherheitseigenschaften der verwendeten Netzwerk-Protokolle sollten dokumentiert sein (siehe Tabelle 1: Beispiel für Kommunikationsübersicht).

Die umgesetzten Härtungsmaßnahmen sind zu dokumentieren, auf Ihre Wirksamkeit zu prüfen und falls erforderlich, anzupassen.

4.5.4 Audit Trails für Nachverfolgung

Audit Trails (Logbücher ggf. mit Signatur) dienen der Protokollierung von Werteänderungen und System-ereignissen und können im Fehlerfall die System- bzw. Datenwiederherstellung stark vereinfachen.

Die Logbücher müssen bei der Inbetriebnahme möglicherweise aktiviert und konfiguriert werden. Sie sollten zumindest alle Bedieneraktionen (z.B. Facility Manager, Servicetechniker), Änderungen an den Daten sowie Schalt- und Einstellaktionen aufzeichnen.

Die jeweiligen Datenschutzbestimmungen sind zu berücksichtigen.

Projektabhängig ist die Art und Dauer der Archivierung der Logbücher festzulegen.

4.5.5 Arbeitsvorschriften/Verhaltensanweisungen

Basierend auf der Risikoanalyse (siehe Abschnitt 4.2) sind vom Errichter Arbeitsvorschriften und Verhaltens-anweisungen zum dauerhaften Erhalt der IT-Sicherheit zu erstellen und dem Betreiber zu übergeben.

Abschließende und getestete Arbeitsvorschriften/Verhaltensanweisungen Standard Operating Procedure - SOP) betreffend IT-Sicherheit sollten ab Beginn des Anlagebetriebs auf zwei Ebenen vorhanden sein:

1) SOP Normalbetrieb, welche sicherstellen, dass alle Sicherheitselemente dauerhaft funktionsfähig und auf dem neuesten Stand gehalten werden.

2) SOP Störfall welche die Abläufe und Informationen für die Aufklärung eines Störfalls oder möglichen Angriffs, Schadensbegrenzung und -bewältigung festlegt.

Die SOP's bestehen z.B. aus:

– Arbeitsabläufen

– Checklisten

– Erinnerungsfunktionen

Sie sorgen bei Einhaltung dafür, dass alle sicherheitsrelevanten Elemente gepflegt werden.

Die Checklisten für den Störfall sollten Informationen über die einzuhaltenden Meldewege, Rufnummern, Eskalationsstufen, Sofortmaßnahmen etc. enthalten.

4.5.6 Engineering Software/Werkzeuge

Bei allen Engineering Werkzeugen, die an die GA zur Inbetriebnahme angeschlossen werden, muss ein aktueller Malwareschutz installiert sein und die Systeme über aktuelle Patchlevel verfügen. Sollte dies aus technischen Gründen nicht möglich sein, müssen anderen geeignete Schutzmaßnahmen getroffen werden.

Vor dem Einsatz sind mobile Datenträger, Installationsmedien und Notebooks auf bekannte Schadsoftware zu prüfen.

4.5.7 Dokumentation

Die Dokumentation der IT-sicherheitrelevanten Maßnahmen muss aktuell und verfügbar sein.

Es sind auch alle deaktivierten physischen Kommunikationsschnittstellen, Protokolle und Zugänge bzw. Zugriffsmöglichkeiten zur GA zu dokumentieren.

Die Modellbezeichnung der verwendeten Komponenten, deren Einbauort sowie deren Versionsstände und MAC-Adressen sind zu dokumentieren.

Bei der Behandlung eines Sicherheitsvorfalls und bei einem Wechsel des Betreibers oder des verantwortlichen Personals ist ein Überblick über die Netzwerkarchitektur, sowie über die verwendeten Komponenten und deren Konfiguration unerlässlich.

4.5.8 Betreiberinformation/-schulung

Betreiber sind für die korrekte Bedienung aller Sicherheitseinrichtungen der Anlage vom Anlagenerrichter grundsätzlich zu schulen.

Dem Betreiber sind die potenziellen Risiken der IT-Sicherheit zu vermitteln und mögliche Gefahren aufzuzeigen.

4.5.9 Backup / Restore

Die Konfiguration von Systemen sollte gesichert werden, um ein schnelles Wiedereinspielen einer fehlerfreien Version zu ermöglichen (Rollback). Rollback-Tests sollten auf einem Testsystem eingerichtet oder während Wartungsfenstern durchgeführt werden. Die Konfigurationen sollten zentral gespeichert werden (siehe 4.6.6).

4.5.10 Abnahmetest

Die Konfiguration sollte mindestens vor Inbetriebnahme eines Systems getestet werden. Es ist zu prüfen, ob die Systeme gemäß den Vorgaben konfiguriert sind.

Für die Tests sollte eine Testspezifikation erstellt werden, Die Testdurchführung sollte in einem Testbericht dokumentiert werden. Abweichungen von den Vorgaben sollten behoben werden.

Sofern bei der Implementierung und/oder Übergabe der Anlage Schwachstellen entdeckt werden, ist dies zu dokumentieren.

4.6 Betrieb

Mit der Übergabe/Abnahme übernimmt der Betreiber die Verantwortung für den sicheren Betrieb der GA.

Das Informations-Sicherheitskonzept und alle installierten Elemente sollten regelmäßig vom Betreiber hinsichtlich der IT-Sicherheit bewertet und Anpassungen an den Stand der Technik vorgenommen oder veranlasst werden (siehe VDMA 24186-4).

Das Benutzerverhalten ist für die IT-Sicherheit einer GA maßgeblich verantwortlich.

Über die gesamte Lebensdauer müssen alle involvierten Stellen ihre sicherheitsrelevanten Aufgaben erfüllen.

Für den Erhalt der IT-Sicherheit sollten zumindest folgende Maßnahmen durchgeführt werden.

4.6.1 Arbeitsvorschriften/Verhaltensanweisungen

Die vom Errichter übergebenen Arbeitsvorschriften und Verhaltensanweisungen zum dauerhaften Erhalt der IT-Sicherheit, sollten vom Betreiber angewendet und in die vorhandenen Prozesse integriert werden.

Arbeitsvorschriften und Verhaltensanweisungen sollten regelmäßig überprüft und an den Stand der Technik angepasst werden.

Jedes externe System und jeder externe Datenträger sollte vor der Verbindung mit einem TGM-System und vor der Datenübertragung auf Schadsoftware geprüft werden.

Änderungen mit Auswirkungen auf die IT-Sicherheit sollten immer angekündigt und mit allen beteiligten Gewerken, Betreiber- und Nachfrageorganisationen abgestimmt werden. Außerdem sollten Regelungen für den Fall getroffen werden, dass ein Rückbau von Änderungen mit fehlerhaftem Ergebnis nicht oder nur mit hohem Aufwand möglich ist.

4.6.2 Benutzerinformation/-schulung

Benutzer sind für die korrekte Bedienung aller Sicherheitseinrichtungen der Anlage grundsätzlich zu schulen.

Den Benutzern sind die potenziellen Risiken zu vermitteln und mögliche Gefahren aufzuzeigen.

Benutzer sind regelmäßig über das Thema IT-Sicherheit zu informieren. Auffrischungen des Wissens helfen, das Thema IT-Sicherheit auch nach längerer Zeit ohne Vorfälle dauerhaft hoch zu halten. Neue Mitarbeiter müssen eingewiesen werden.

4.6.3 Benutzername/Passwort

Jeder Benutzer sollte einen individuellen Benutzernamen und Passwort verwenden.

Insbesondere für das Audit Trail sind individuelle Benutzer mit eigenem Passwort Voraussetzung.

Die Benutzer sind gefordert, sichere Passwörter zu verwenden. Auf keinen Fall sollten Passwort Elemente aus naheliegenden Inhalten, wie z.B. Namen, Namen des Partners/der Kinder, Geburtsdatum enthalten (siehe BSI Empfehlungen).

4.6.4 Security-relevante Updates/Upgrades

Alle Geräte und Programme, insbesondere die PCs, deren Malwareschutz, die Kommunikationseinrichtungen wie Router, VPN-Geräte etc. sollten regelmäßig mit den verfügbaren und freigegebenen Security-relevanten Updates und Upgrades aktualisiert werden (siehe VDMA 24186-4). Deren Authentizität und Integrität muss im Rahmen der Installation erfolgreich geprüft werden.

Für alle Systeme des TGM sowie die Systeme, die durch das TGM betrieben werden, sollte bei der Beschaffung sichergestellt werden, dass diese angemessen gehärtet werden können und insbesondere sicherheitsrelevante Updates möglichst für die geplante Nutzungsdauer bereitgestellt werden.

Systeme, für die keine sicherheitsrelevanten Updates verfügbar sind, sollten nach Bekanntwerden von Schwachstellen nicht mehr genutzt werden.Wenn dies nicht möglich ist, sollten die betroffenen Systeme mit den Mitteln der Netzsegmentierung separiert und die Kommunikation kontrolliert und reglementiert werden.

Konfigurationsänderungen sollten dokumentiert und allen Beteiligten an Betriebs- und Serviceprozessen (Entstörung, Rufbereitschaft, Wartungen etc.) bekannt gemacht werden, insbesondere Änderungen der Zugangsmechanismen oder der Passwörter.

4.6.5 Periodische Security-Tests

Die Sicherheitsmaßnahmen sollten in vordefinierten Intervallen überprüft und getestet werden. Penetrationtests werden empfohlen.

Auch die Abläufe nach einem Angriff/Störungsfall sollten regelmäßig geübt werden

Testspezifikationen (siehe 4.5.10) sollten regelmäßig und zusätzlich bei Bedarf geprüft und gegebenenfalls aktualisiert werden,um dem aktuellen Stand der Technik zu entsprechen und auch neueste Erkenntnisse abdecken zu können.

Außerdem sollte regelmäßig und zusätzlich bei Bedarf geprüft werden, ob die Systeme gemäß den Vorgaben konfiguriert sind. Die Ergebnisse sollten nachvollziehbar dokumentiert werden. Abweichungen von den Vorgaben sollten behoben werden.

4.6.6 Back-ups

Back-ups (z.B. Anlagenprogrammierung, Konfiguration, Konfigurationsänderungen, Betriebsdaten) sollten regelmäßig erstellt werden und müssen auf ihre korrekte und vollständige Ausführung überwacht werden. Periodisch müssen sie auf ihre Brauchbarkeit getestet werden. Das Back-up sollte dazu geeignet sein die gesamt GA wiederherzustellen.

Die Back-ups sind durch den Betreiber vor unberechtigten Zugriff zu schützen. Da die Back-up-Dateien normalerweise auch Kopien von hochsensiblen Daten enthalten, müssen diese verschlüsselt oder an einem zuverlässig geschützten Ort aufbewahrt werden (siehe VDMA 24186-4).

4.6.7 Dokumentation

Engineering Dokumente wie Netzwerktopologien, IT-Sicherheitskonzepte etc., müssen (inkl. all ihrer Kopien) zugangsgeschützt aufbewahrt werden.

4.7 Fern-Übertragung /-Services

GA-Systeme erfordern oftmals eine externe Unterstützung durch den Hersteller oder weitere Dienstleister oder übertragen Monitoring-Daten an externe Dienstleister.

GA-Systeme, die kritische Infrastrukturen steuern und regeln, erfordern zusätzliche kurze Reaktions- und Wiederherstellungszeiten. Dies führt oftmals zur Einrichtung von Fernwartungs-Zugängen über öffentliche Netze als Kommunikationsträger. Diese Zugänge dürfen den erreichten IT-Schutzlevel des GA-Systeme nicht oder nur unerheblich vermindern. Eine Abwägung der einzelnen Randbedingungen mit den erreichbaren Vorteilen, bestehenden Risiken und dem jeweiligen Gefährdungspotentialen ist dabei im jeweiligen Anlagenfall durchzuführen.

Die Grundlagen zur Inanspruchnahme von Fernservices von externen Dienstleistern und Herstellern sind vertraglich mit diesen Anbietern und dem Betreiber der GA Systeme zu regeln. Dabei sind auch die geltenden Datenschutzbestimmungen u beachten.

Bei einem Fern-Service ist zu beachten, dass gesicherte Kommunikationswege genutzt werden. VPN Verfahren sind hierzu geeignet.

Es ist dabei sicherzustellen, dass nur vereinbarte Daten aus vereinbarten Systemen übertragen werden.

Bei einem laufenden Fernzugriff muss es für den Betreiber der GA Systeme jederzeit die Möglichkeit geben, diesen abzubrechen.

4.8 Rückbau

Beim Rückbau oder Ersatz von GA Komponenten und Systemen müssen sensible Daten auf diesen Geräten sicher und zuverlässig gelöscht werden.

Literaturhinweise

Dr. Thomas Porter, The Perils of Deep Packet Inspection, SecurityFocus.com, veröffentlicht 2005-01-11, aktualisiert 2010-10-19]

DSGVO Datenschutz-Grundverordnung (EU) 2016/679 (https://dsgvo-gesetz.de/)

BSI Richtlinie TR-02102 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" Version: 2020-01 (https://www.bsi.bund.de)

bsi Grundschutzkompendium: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html