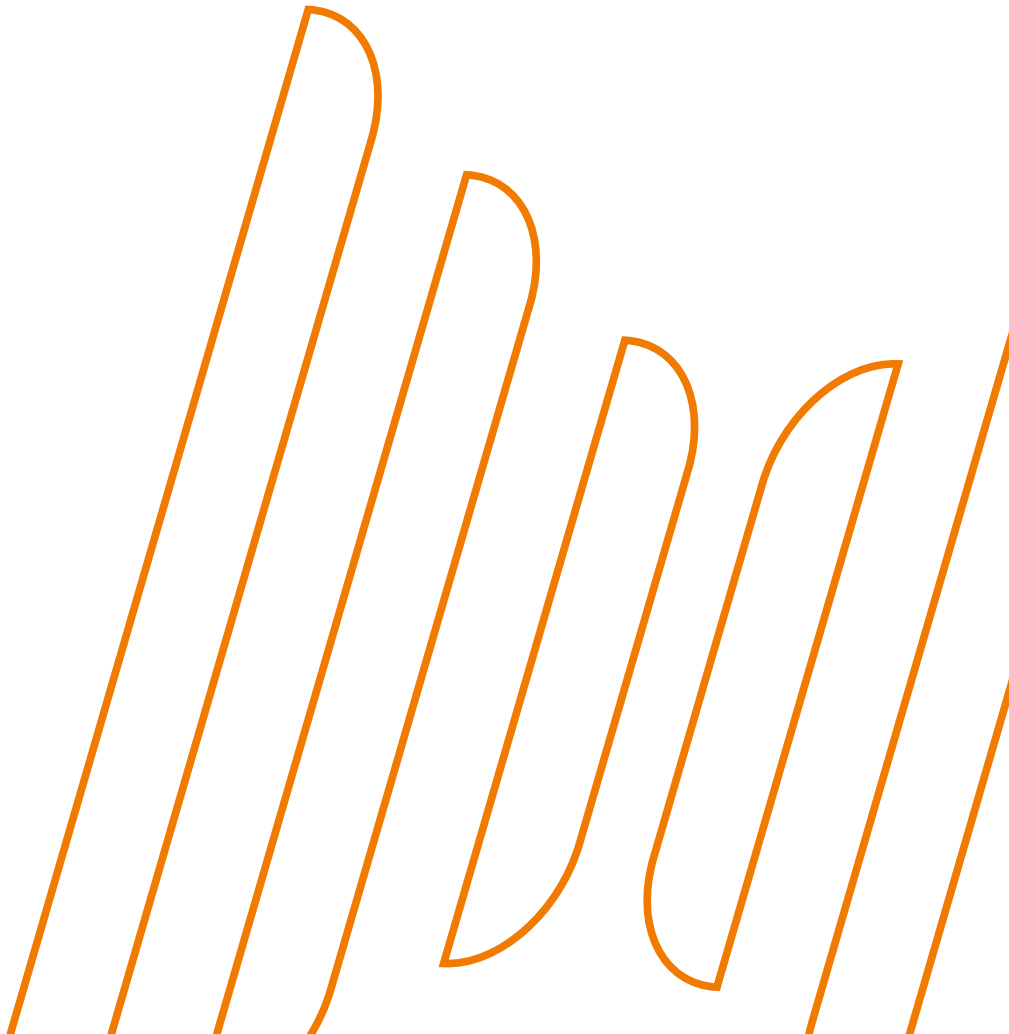
VDMA

FACHVERBAND AUTOMATION + MANAGEMENT FÜR HAUS+ GEBÄUDE

EMPFEHLUNG

Empfehlung für Ausschreibungstextmodule in Anlehnung an das VDMA EB 24774 für die IT-Sicherheit in der Gebäudeautomation



März 2026

Vorwort

Bei den in diesem Dokument gelisteten Textbausteinen handelt es sich um exemplarisch ausformulierte Textbausteine für Ausschreibungstexte für IT-Sicherheitsanforderungen basierend auf dem VDMA Einheitsblatt 24774 "IT-Sicherheit in der Gebäudeautomation", die je nach Projektanforderungen beliebig kombiniert und inhaltlich angepasst werden können. Das VDMA-Einheitsblatt 24774 dient als praxisorientierter Leitfaden zur Gewährleistung der IT-Sicherheit in der Gebäudeautomation (GA).

Diese Empfehlung erhebt weder einen Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Sie darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen.

Der Inhalt dieser Empfehlung wurde sorgfältig recherchiert und zusammengestellt, ersetzt aber nicht die Rechtsberatung im Einzelfall. Für die Richtigkeit und Vollständigkeit sowie für zwischenzeitlich eingetretene Änderungen wird keine Haftung übernommen.

Einführung

Die gelisteten Ausschreibungstextbausteine auf Basis des VDMA Einheitsblattes 24774 können von Planern und Bauherren genutzt werden, weil sie die Brücke zwischen dem theoretischen Einheitsblatt und der praktischen Umsetzung schlagen.

Auftragnehmer haben die Aufgabe angemessene organisatorische und technische Maßnahmen zu treffen, um eine Gebäudeautomation vor Datenmanipulation, Datenverlust oder Ausfall und deren Folgen zu schützen.

Die Anforderungen für die IT-Sicherheit in der Gebäudeautomation werden in einer individuellen Risikoanalyse definiert. Diese Anforderungen müssen vom Bauherrn, dem Planer oder dem Betreiber vorgegeben werden.

Der Auftragnehmer ist verantwortlich für die Erarbeitung eines Sicherheitskonzeptes für die Gebäudeautomation und alle betreffenden Anwendungen.

Ziel des Sicherheitskonzeptes ist es, eine Gefährdungsübersicht, Risikoeinschätzung, Risikobehandlung zu erstellen und durch Sicherheitsmaßnahmen zu behandeln. Zwingender Bestandteil des Sicherheitskonzeptes muss ein Wiederherstellungskonzept

nach Eintritt eines Schadensfalls sein, um die Anlagen-Stillstands-Zeit soweit möglich zu reduzieren.

Die Sicherheit der Gebäudeautomation soll den Empfehlungen VDMA Einheitsblattes 24774 „IT-Sicherheit in der Gebäudeautomation“, und deren Verweise in seiner aktuellen Fassung, für die Errichtung und den Betrieb der Anlage entsprechen.
Der Auftragnehmer sollte branchenübliche Standards, Prozesse und Methoden in Übereinstimmung mit Standards des BSI Grundschutz Kompendium mit den Hinweisen zur Infrastruktur Gebäudeautomation (INF.14) und Gebäudemanagement (INF.13) sowie DIN EN ISO 16484 *Gebäudeautomation, VDMA 24186-4, Leistungsprogramm für die Wartung von technischen Anlagen und Ausrüstungen in Gebäuden* anwenden.

Die Datenschutz-Grund-Verordnung – DSGVO zum Schutz personenbezogener Daten muss bei dem Maßnahmenkonzept berücksichtigt werden.

Die zu erarbeitenden Maßnahmen zur Prävention und Schadenabwehr umfassen den gesamten Lebenszyklus der Gebäudeautomationsanlage wie Planung, Realisierung, Nutzung, Rückbau. Ein gesamtheitliches IT-Sicherheitskonzept erfordert die Einbindung aller Beteiligten der vier Phasen Planung, Ausführung, Betrieb und Rückbau.

Das VDMA Einheitsblattes 24774 „IT-Sicherheit in der Gebäudeautomation“ steht jedem Interessierten kostenfrei auf der VDMA Webseite (www.VDMA.eu/AMG) zur Verfügung.

Empfehlungen für Ausschreibungstexte basierend auf dem VDMA Einheitsblatt 24774 " IT-Sicherheit in der Gebäudeautomation"
Die Nummerierung der Kapitel beziehen sich auf die Kapitel des EB 24774-2023.

Hinweis:

Im VDMA Einheitsblattes EB 24774 sind viele Anforderungen der IT-Sicherheit als Empfehlung für die Gebäudeautomation formuliert. Wenn eine IT-Sicherheits-funktionalität gemäß der Risiko-/Schwachstellenanalyse in dem jeweiligen Bauprojekt als erforderlich angesehen wird, kann der folgende Ausschreibungstextbausteine mit verpflichtender Formulierung verwendet werden.

4.2 Risiko-/Schwachstellenanalyse

Gemäß dem VDMA EB 24774 wird für Gebäudeautomationssysteme im Nichtwohnbereich eine Risikoanalyse als Basis für die Auslegung der angemessenen Schutzmaßnahmen empfohlen.

Der Bieter ermittelt im Rahmen der Risikoanalyse in Abstimmung mit dem Bauherren/Vertreter des Bauherren den projektspezifische Schutzbedarf für die Gebäudeautomation.

Der Bieter erstellt zu diesem Schutzbedarf die geeigneten Sicherheitsvorkehrungen und verfasst das IT Sicherheitskonzept Gebäudeautomation.

Im Detail werden als Prozess zur Risikoanalyse der IT-Sicherheit der Gebäudeautomation folgende Schritte vorgesehen:

- Gefährdungsübersicht (Erstellung einer Liste von möglichen elementaren Gefährdungen sowie Ermittlung zusätzlicher Gefährdungen, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario ergeben)
- Risikoeinstufung (Risikoeinschätzung (Ermittlung von Eintrittshäufigkeit und Schadenshöhe), Risikobewertung (Ermittlung der Risikokategorie))
- Risikobehandlung (Risikovermeidung, Risikoreduktion (Ermittlung von Sicherheitsmaßnahmen), Risikotransfer, Risikoakzeptanz)
- Sicherheitskonzept (Integration der aufgrund der Risikoanalyse identifizierten zusätzlichen Maßnahmen). Zwingender Bestandteil des Sicherheitskonzeptes muss ein Wiederherstellungskonzept nach Eintritt eines Schadensfalls sein, um die Anlagenstillstandszeit und Datenmanipulation und Datenverlust soweit möglich zu reduzieren.

Gerade bei den Schritten der Risikoeinstufung, Risikobehandlung und bei dem Sicherheitskonzept müssen die Besonderheiten von OT (Betriebstechnologie Gebäudeautomation) im Vergleich zur IT (Informationstechnologie) berücksichtigt werden.

Dienstleistung Erstellung der Risiko-/Schwachstellenanalyse, Erstellung oder Erweiterung des IT Sicherheitskonzept Gebäudeautomation inklusive der Maßnahmenvorgaben gemäß Vortext: pauschal oder nach Stunden

4.3.1 Zugangsrechte-System/Passwortschutz

Gemäß dem VDMA EB 24774 wird für die Gebäudeautomationssysteme im Nichtwohnbereich das Zugangsrechte-System/Passwortschutz umgesetzt.

Alle Geräte und Softwareprodukte des Bieters die über Benutzerzugänge (Webserver, Konfigurationszugänge etc.) verfügen, müssen mit einem konfigurierbaren Zugangsrechtesystem mit Authentisierungsmechanismus (z.B. Passwortschutz) ausgestattet sein. Die Komponenten sind entsprechend dem Schutzkonzept so zu konfigurieren, dass Passwortsicherheit, ggf. periodische Passworterneuerung, Autologout, Sperrung nach erfolglosen Login-Versuchen umgesetzt wird.

Die Datenschnittstellen, welche die Geräte/Softwareprodukte für die Kommunikation mit ihren Datenquellen verwenden, sind mit der im Schutzkonzept angegebenen verifizierten Identifikation vor unerlaubtem Zugriff zu schützen. Bei der Kommunikation mit der Feldebene ist dies, soweit es das Protokoll in der Feldebene zulässt, weiterzuführen.

Standard-Passwörter für voreingerichtete Benutzer müssen nach der Inbetriebnahme, spätestens im Rahmen der Übergabe/Abnahme, gemäß dem Schutzkonzept angepasst werden. Komponenten, die keinen Zugangsschutz beinhalten, werden entsprechend dem Schutzkonzept dann abgeschaltet oder durch zusätzliche Maßnahmen geschützt. Alle voreingerichteten Benutzerberechtigungen müssen dokumentiert sein.

Dienstleistung Umsetzung der Zugangsrechte-System/Passwortschutz gemäß Sicherheitskonzept gemäß Vortext: pauschal oder nach Stunden.

4.3.2 Verschlüsselte Kommunikation zum Nutzer (Webserver)

Der Bieter muss sicherstellen, dass die Netzwerkkommunikation von Feld-, Automations- und ggf. Managementgeräten der Gebäudeautomation zu den Webservern und ihre Konfigurationsschnittstellen eine TLS -gesicherte Kommunikation nach Stand der Technik (siehe BSI Richtlinie TR-02102) unterstützt. Komponenten, die keine gesicherte Kommunikation beinhalten, werden entsprechend dem Schutzkonzept spätestens nach der Inbetriebnahme abgeschaltet oder durch zusätzliche Maßnahmen geschützt.

Dienstleistung Umsetzung der Verschlüsselung gemäß Vortext: pauschal oder nach Stunden (für die gelieferten Geräte/ für das komplette System)

4.3.3 Gehärtete Geräte und Software

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich bei netzwerkfähigen Komponenten geeignete Vorgaben für die Härtung.

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. Wenn das ab Auslieferung nicht möglich ist, dann muss dieser Zustand spätestens bei der Inbetriebnahme hergestellt werden.

Der Bieter hat am Ende der Inbetriebnahme alle unbenutzten Dienste, physikalische Zugänge, Benutzerkonten, Protokolle, Schnittstellen, nichtgenutzte Ports und Programme bewertet und entfernt oder deaktiviert. Nur die für den Betrieb notwendigen Elemente dürfen auf den Geräten verbleiben. Besitzt eine Komponente Anwendungs-, Wartungs- oder Entwicklungsschnittstellen, über die Informationen unverschlüsselt übertragen werden, müssen diese spätestens nach der Inbetriebnahme deaktiviert werden. Standardmäßig eingerichtete bzw. vom Hersteller gesetzte Passwörter müssen gewechselt werden, wenn der Zugang hierüber nicht deaktiviert werden kann.

Wenn eine Härtung an einem Gerät selber nicht möglich ist, sollten deren nicht benötigte Dienste und Ports über eine Firewall eingeschränkt werden. Die entsprechenden Geräte sollten dann in einem separierten Netzwerksegment betrieben und deren Kommunikation kontrolliert werden.

Die Härtungsmaßnahmen müssen dokumentiert und dem Bauherren übergeben werden.

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

Dienstleistung Nachhärten der GA-Komponenten gemäß Vortext: pauschal oder nach Stunden

4.3.4 Audit-Trail-Funktionen

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich bei netzwerkfähigen Komponenten mit Benutzerverwaltung eine Protokollierung und Nachverfolgung von relevanten Systemereignissen und Benutzeraktivitäten wie Wertänderungen.

Der Bieter stellt sicher, dass gemäß dem Schutzkonzept relevante Statusänderungen von GA-Komponenten, Benutzeraktivitäten sowie manuelle Werteänderungen, protokolliert und optional kommentiert werden. Die Protokollierungsdaten sollten an einer zentralen Stelle gespeichert werden. Es muss sichergestellt sein, dass die aufgezeichneten Protokollierungsdaten nicht

verändert oder in einer vom AG festgelegten Frist von mindestens 6 Monaten gelöscht werden können.

Die Protokollierungsdaten müssen berechtigten Personen zur Auswertung verfügbar gemacht werden.

Sofern eine als relevant definierte Anwendung über eine solche Protokollierungsfunktion verfügt, muss diese Funktion benutzt werden. Eine Protokollierung von Benutzerdaten muss DSGVO konform erfolgen.

Abhängig von der spezifischen Risikoanalyse kann diese Funktionalität bei Gebäuden mit erhöhtem Schutzbedarf als verpflichtend gefordert werden.

Dienstleistung Implementierung eines GA-Audit-Trails gemäß Vortext: pauschal oder nach Stunden.

4.3.5 Security-relevante Updates

Gemäß dem VDMA EB 24774 wählt der Bieter ein Gebäudeautomationssystem aus, das vom Hersteller regelmäßig an die aktuelle IT-Anforderungen angepasst und auf Schwachstellen überprüft wird. Erkannte Sicherheitslücken müssen durch das Einspielen von Sicherheitsupdates geschlossen werden können. Dazu stellt der ausgewählte Hersteller geeignete Verfahren und Prozesse zur Verfügung, um Anlagenbetreiber über Sicherheitslücken zu informieren, gegebenenfalls in einem strukturierten, maschinenlesbaren Format, das leicht automatisch zu verarbeiten ist.

Dienstleistung Bereitstellung regelmäßige Updates gemäß Vortext: pauschal oder nach Stunden

4.4 Projektierungs-Ebene (Ausführungsplanung IT-Sicherheit)

Gemäß dem VDMA EB 24774 wird der Bieter im Rahmen der Projektierung der Gebäudeautomation die geplanten oder bestehenden Anlagen umfassend bewerten und in die Bearbeitung integrieren.

Der Bieter integriert die Vorgaben der Bauherren und Fachplaner sowie der für IT und OT verantwortlichen Personen, die maßgeblich an der Planung und Ausführung beteiligt sind. Sie legen die technischen Anforderungen fest, die die Grundlage für die Umsetzung der Sicherheitsmaßnahmen bilden. Zudem müssen alle Anforderungen, die sich aus einem TGM-Konzept ergeben, in die Planung und Umsetzung einfließen.

Je nach Art der Anlage und des Gebäudes sind folgende Punkte zu definieren und zu dokumentieren:

1. Netzwerktopologie: Erstellung einer detaillierten Dokumentation der Netzwerke und ihrer Segmente.
2. Schutzmaßnahmen:
   - An Netzsegmentübergängen und Zugangspunkten (LAN, WLAN, WAN, physischer Zugang).
   - An Schnittstellen zu anderen Gewerken.
3. Sicherheitsmaßnahmen: Festlegung der erforderlichen Sicherheitsmaßnahmen, die auf den Rechnern und Servern der Management-Ebene installiert werden müssen.
4. Risiko-/Schwachstellenanalyse: Identifikation weiterer Maßnahmen basierend auf der durchgeführten Risiko- und Schwachstellenanalyse.
5. Inbetriebnahme- und Schnittstellenmanagement: Entwicklung eines umfassenden Managementplans für die Gebäudeautomation.
6. Havarie Management: Strategien zur Handhabung von Vorfällen infolge eines Angriffs.
7. Kommunikationssicherheit:
   - Einsatz sicherer Protokolle für die Kommunikation von GA-relevanten Komponenten, die auf Ethernet und IP basieren, insbesondere über nicht-vertrauenswürdige Netzsegmente (integritätssichere Datenübermittlung).
   - Verschlüsselung der Kommunikation über Ethernet und IP zwischen GA-Systemen außerhalb vertrauenswürdiger Netzsegmente unter Verwendung aktueller Verschlüsselungsmechanismen.
8. Identitäts- und Berechtigungsmanagement: Implementierung eines Systems, das die Anforderungen der Gebäudeautomation gemäß dem Schutzkonzept umsetzt.
9. Abnahmetest der IT-Sicherheit: Durchführung von Tests zur Überprüfung der IT-Sicherheit.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.4.1 Getrennte GA-IP-Netzwerke (optional, wenn OT und IT in einem Netz geführt werden)

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich eine Netzwerktrennung. Der Bieter muss zur Sicherstellung der IT-Sicherheit für die Gebäudeautomation (GA), eine Trennung der GA-IP-Netzwerke von anderen Netzwerken vorsehen.

Um die Integrität und Verfügbarkeit der GA-Systeme zu gewährleisten, wird gefordert, dass jegliche Kommunikation zwischen GA-Systemen und anderen IT-Systemen streng kontrolliert und reglementiert wird. An allen Übergängen der Segmentierung sind geeignete Sicherheitskomponenten, mindestens mit Firewall-Funktion, zu implementieren.

GA-Netze mit erhöhtem Schutzbedarf sollen als physisch getrennte Zonen realisiert werden.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden

4.4.2 Mit Firewalls gesicherte Netzwerke/Segmente

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich eine Absicherung der Netzwerkzugänge. Der Bieter hat sicherzustellen, dass alle Netzwerkzugänge durch Firewalls (FW) gegen unberechtigte Zugriffe geschützt sind. Um die Sicherheit der Systeme zu gewährleisten, sind Segmente mit unterschiedlichem Schutzbedarf ausreichend voneinander zu trennen.

Im Rahmen der Projektierung und Inbetriebnahme müssen die Firewalls entsprechend dem Schutzkonzept konfiguriert werden, um eine optimale Integration in die Gebäudeautomation zu gewährleisten.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

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

Gemäß dem VDMA EB 24774 hat der Bieter sicherzustellen, dass abgesetzte Stationen, die sich außerhalb des LAN befinden, sowie Inseln und Fern-Services über eine geschützte Kommunikation mit dem Gebäudeautomationssystem (GA-System) verbunden werden. Hierbei kommen die Technologien des Schutzkonzeptes wie VPN oder HTTPS zum Einsatz, um die Integrität und Vertraulichkeit der Daten zu gewährleisten. Zusätzlich wird gefordert, den Zugriff dieser abgesetzten Stationen auf das GA-System durch geeignete Firewall-Regeln auf das notwendige Minimum zu beschränken.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden

4.4.4 Switches/Router mit Sicherheits-Funktionen

Im Rahmen der gemeinsamen Nutzung einer Netzwerkinfrastruktur durch die Gebäudeautomation (GA) und andere GA-fremde Nutzer ist gemäß dem VDMA EB 24774 der Einsatz von Switchen und Routern mit integrierten Sicherheits-Funktionen gefordert. Diese Geräte tragen zur Verbesserung der Sicherheit der an diesem gemeinsam genutzten Netzwerk angeschlossenen GA-Komponenten bei, indem sie den Datenverkehr zu jedem einzelnen

Teilnehmer filtern. Der Switch oder Router gewährleistet, dass jeder Teilnehmer ausschließlich die Datenpakete erhält, die für ihn bestimmt sind. Höher entwickelte Switches haben die Fähigkeit, ausgewählte Teilnehmer eines Netzwerks, wie beispielsweise die GA-Teilnehmer, in einem VLAN (Virtual Local Area Network) zusammenzufassen. Dadurch kommunizieren diese innerhalb ihres eigenen, virtuellen Netzwerks und sind für andere Netzwerkteilnehmer nur sichtbar und erreichbar, wenn dies explizit im Netzwerkkonzept eingeplant und umgesetzt wird. Zusätzlich besteht die Anforderung, die Switches manuell mit White Lists und Black Lists zu konfigurieren. In diesen Listen wird bei der Inbetriebnahme festgelegt, welche Geräte (basierend auf der MAC-Adresse) an welchem Port angeschlossen werden dürfen und welche nicht. Dies erschwert den Anschluss von nicht autorisierten oder fremden Geräten an das GA-Netzwerk erheblich.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden

4.4.5 Funknetzwerke

Beim Betrieb von Funknetzwerken bei der Gebäudeautomation ist gemäß VDMA EB 24774 zu beachten, dass diese aufgrund des einfachen physischen Zugangs besonders anfällig gegenüber potenziellen Angreifern sind. Daher ist es unerlässlich, die einzusetzenden Technologien auf Basis einer umfassenden Risikoabschätzung auszuwählen.

Für Geräte, die über WLAN (Wireless LAN) mit dem GA-Netzwerk verbunden werden, ist der Einsatz eines WLAN-Access-Points mit aktueller Verschlüsselungstechnik, vorzugsweise nach dem WPA3-Standard, zu verwenden. Gemäß den Vorgaben des BSI Grundschutz dürfen kryptographische Verfahren, die als unsicherer als WPA2 gelten, nicht mehr verwendet werden. WPA3 wird als sicher angesehen, sofern ausreichend lange und komplexe Passwörter verwendet werden und die WPS-Funktion deaktiviert ist.

Für den Betrieb von Kleingeräten, die in der Regel batteriebetrieben sind und in einem WPAN (Wireless Personal Area Network) eingesetzt werden, sollte eine IP-basierte Technologie zum Einsatz kommen. Diese Technologie muss die Verwendung von Standard IT-Sicherheitsprotokollen, wie beispielsweise TLS, unterstützen.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.4.6 Daten- und Zeit-Synchronisierung

Gemäß dem VDMA EB 24774 ist für das Gebäudeautomationssystem sicherzustellen, dass die visualisierten Informationen hinsichtlich Zeit, Ort, Wert, Zustand oder Ereignis klar erkennbar sind und auf planmäßig erhaltenen Daten basieren. Informationen, die simulierte oder „eingefrorene“ Werte anzeigen, müssen entsprechend dem Schutzbedarf der TGA-Anlagen (Technische Gebäudeausrüstung) entweder deutlich erkennbar sein oder einen Alarm auslösen.

Des Weiteren ist es erforderlich, dass alle im GA-System angebundenen Komponenten sowie TGA-Anlagen eine synchrone Uhrzeit verwenden. Dies ist entscheidend, um ein automatisiertes Messen, Steuern und Regeln zu gewährleisten. Auch miteinander verbundene GA-Systeme müssen eine einheitliche Zeitsynchronisation aufweisen.

Sollte sich das GA-System über mehrere Gebäudekomplexe oder Liegenschaften erstrecken, ist sicherzustellen, dass die Zeitsynchronisation durch genormte Protokolle für alle beteiligten Gebäude gewährleistet wird.

Dienstleistung Erfüllung der Anforderungen gemäß Vortext: pauschal oder nach Stunden

4.4.7 Schutz vor Schadsoftware

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich ein umfassendes Konzept zum Schutz vor Schadsoftware auf den beteiligten Servern und Computern. Neben dem Netzwerkschutz muss durch den Bieter während der Projektierungsphase festgelegt werden, wie dieser Schutz konkret umgesetzt wird. Um die Wirksamkeit des Schutzes langfristig zu gewährleisten, ist zudem ein praktikables Aktualisierungskonzept zu definieren. Wenn auf einem System kein Virenschutzprogramm eingesetzt werden kann, beispielsweise aufgrund begrenzter Ressourcen oder spezifischer Echtzeitanforderungen, sind geeignete alternative Schutzverfahren zu implementieren. Der Schutz vor Schadsoftware soll die Auswirkungen von bekannten Bedrohungen wie Computerviren, Computerwürmern und Trojanischen Pferden verhindern und diese, wenn möglich, beseitigen. Da nur bekannte Schadsoftware erkannt werden kann, ist eine kontinuierliche Aktualisierung der Schutzmaßnahmen unerlässlich. Jedes externe System sowie jeder externe Datenträger muss vor der Verbindung mit dem GA-System und vor der Datenübertragung auf Schadsoftware geprüft werden, um die Integrität und Sicherheit des Systems zu gewährleisten.

Dienstleistung Erfüllung der Anforderungen gemäß Vortext: pauschal oder nach Stunden

4.4.8 Back-up Konzept inkl. Recovery-Anweisungen

Im Falle eines Angriffs oder eines Ausfalls der Gebäudeautomation (GA) wird die Funktionsfähigkeit des betroffenen Gebäudes erheblich beeinträchtigt. Um den Betrieb und die Nutzbarkeit sicherzustellen, ist gemäß dem VDMA EB 24774 gefordert, ein umfassendes Back-up Konzept zu entwickeln. Dieses Konzept muss eine klar definierte Vorgehensweise sowie eine detaillierte, getestete und geübte Schritt-für-Schritt Recovery-Anweisung beinhalten.

Die Back-up Dateien enthalten in der Regel hochsensible Daten, weshalb bereits in der Planungsphase darauf geachtet werden muss, wo diese Daten zuverlässig und sicher aufbewahrt werden. Besonders schützenswert sind Inhalte wie Systemkonfigurationsinformationen, personenbezogene Daten und Daten der Benutzerverwaltung.

Der Anbieter muss in der Lage sein, ein solches Back-up Konzept zu erstellen und die entsprechenden Recovery-Anweisungen zu implementieren. Die Lösung sollte sowohl die Sicherheit der Daten gewährleisten als auch die schnelle Wiederherstellung der Systeme im Notfall ermöglichen.

Dienstleistung Erfüllung der Anforderungen gemäß Vortext: pauschal oder nach Stunden

4.4.9 Physische Anlage/Schaltschranksicherung

Um Angriffe und unbefugte Zugriffe auf die Anlage, die Schaltschränke und die Kommunikationseinrichtungen zu verhindern, ist gemäß dem VDMA EB 24774 eine umfassende physische Sicherung sicherzustellen. Im Rahmen der IT-Sicherheit muss insbesondere die Absicherung der physikalischen Zugangspunkte an den Geräten, Schaltschränken und Kommunikationseinrichtungen gewährleistet werden.

Es ist sicherzustellen, dass sowohl freie als auch belegte Ethernet-, USB- und Konfigurationssteckdosen an PCs, ASn, Routern und weitere Geräten für unberechtigte Personen nicht zugänglich sind. Besondere Aufmerksamkeit sollte alle erreichbaren GA-Elementen beispielsweise den Bediengeräten der Raumautomation gelten, da diese je nach eingesetzter Technik potenzielle Zugangsmöglichkeiten zum Gebäudeautomationsnetzwerk darstellen können.

Für frei zugängliche LAN- oder WLAN-Zugänge sowie kommunikative Systeme, die nicht physisch abgesichert werden können, ist die Implementierung einer Netzzugangskontrolle gemäß IEEE 802.1X oder anderer geeigneter Sicherheitsmechanismen erforderlich.

Frei zugängliche Schnittstellen für temporäre Wartungszwecke, wie beispielsweise USB-Ports an GA-Komponenten, dürfen nur bei Bedarf aktiviert werden, um die Sicherheit der gesamten Anlage zu gewährleisten.

Dienstleistung Erfüllung der Anforderungen gemäß Vortext: pauschal oder nach Stunden

4.5. Inbetriebnahme-Ebene

4.5.1 Anpassung der Berechtigungen

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich bei netzwerkfähigen Komponenten mit Benutzerverwaltung eine Definition und Anpassung der Benutzerberechtigung.

Der Bieter hat den Zugriff zu den netzwerkfähigen Komponenten und Diensten durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer oder Dienste der IT-Systeme abzusichern.

Bei der Inbetriebnahme muss der Bieter für alle betroffenen Geräte, PCs und Systeme der Gebäudeautomation die Benutzer/Benutzergruppen entsprechend ihrer Berechtigung definieren und angelegen. Die Berechtigungen sollten möglichst restriktiv und möglichst individuell vergeben werden. Zugelassene Benutzer, angelegte Benutzergruppen und Rechteprofile sollten geeignet dokumentiert werden. Es müssen die ursprünglichen Standard- oder Default Zugänge durch projektspezifische Zugänge ersetzt werden.

Die Dokumentation der Benutzerberechtigungen muss dem Kunden auf geeignetem Weg vertraulich übergeben werden.

Dienstleistung Anpassen der GA-Berechtigung: pauschal oder nach Stunden

4.5.2 Passwort-Vorgaben/-Ablaufzeit, Autologout

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich bei netzwerkfähigen Komponenten mit Benutzerverwaltung geeignete Vorgaben zur Benutzerauthentifizierung.

Der Bieter muss sicherstellen, dass der Zugriff zu den netzwerkfähigen Komponenten und Diensten durch eine angemessene Identifikation und Authentisierung der zugreifenden Benutzer oder Dienste der IT-Systeme abgesichert ist. Der Bieter muss sicherstellen, dass nur

Berechtigte auf die Komponenten zugreifen können. Eine geeignete Authentifizierung kann gemäß Vorgaben des Sicherheitskonzeptes hierbei über verschiedene Mechanismen wie beispielsweise ein Benutzerlogin mit zugehörigem Passwort erfolgen. Die entsprechenden Komponenten und Dienste der Gebäudeautomation müssen hierbei geeignete Vorgaben für Login und Passworte bieten. Die Vorgaben sollten projektspezifisch anpassbar sein. Hierbei sollte beispielsweise die Komplexität, die minimale Anzahl der Wiederholungen, die automatische Ablaufzeit und die Autologoff-Zeit geändert werden können. Für das Zurücksetzen von Passwörtern muss ein geeigneter Prozess definiert werden. Die Authentifizierungsvorgaben müssen durch organisatorische oder technische Maßnahmen ausreichend bekannt und dokumentiert sein.

Der Bieter hat in Abhängigkeit von der spezifischen Risikoanalyse diese Funktionalität bei Gebäuden mit erhöhtem Schutzbedarf verpflichtend umzusetzen. Die Anforderungen an die Authentifizierungsmechanismen und deren Vorgaben steigen mit dem jeweiligen Schutzprofil des Gebäudes. Abhängig von der spezifischen Risikoanalyse können auch weitergehende Mechanismen bei der Authentifizierung wie Multifaktor- oder biometrische Verfahren gefordert werden.

Dienstleistung Umsetzen der GA-Passwortvorgaben: pauschal oder nach Stunden

4.5.3 Nachhärtung Geräte/PC/Komponenten

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich bei netzwerkfähigen Komponenten geeignete Vorgaben für die Härtung.

Der Bieter muss sicherstellen, dass am Ende der Inbetriebnahme alle unbenutzten Dienste, physikalische Zugänge, Benutzerkonten, Protokolle, Schnittstellen, nichtgenutzte Ports und Programme bewertet und möglichst entfernt oder deaktiviert werden. Nur die für den Betrieb notwendigen Elemente sollten auf den Geräten verbleiben. Besitzt eine Komponente Anwendungs-, Wartungs- oder Entwicklungsschnittstellen, über die Informationen unverschlüsselt übertragen werden, müssen diese spätestens nach der Inbetriebnahme deaktiviert werden. Standardmäßig eingerichtete bzw. vom Hersteller gesetzte Passwörter müssen gewechselt werden, wenn der Zugang hierüber nicht deaktiviert werden kann.

Wenn eine Härtung an einem Gerät selber nicht möglich ist, hat der Bieter deren nicht benötigte Dienste und Ports über eine Firewall einzuschränken. Die entsprechenden Geräte sollten dann in einem separierten Netzwerksegment betrieben und deren Kommunikation kontrolliert werden.

Die Härtungsmaßnahmen sind durch den Bieter zu dokumentieren und an den Betreiber zu übergeben.

Alle aktiven Dienste und Zugänge der GA sind durch den Bieter zu dokumentieren. Die Sicherheitseigenschaften der verwendeten Netzwerk-Protokolle sind vom Bieter aufzuführen und zu dokumentieren. Die umgesetzten Härtungsmaßnahmen sind vom Bieter zu dokumentieren, auf Ihre Wirksamkeit zu prüfen und, falls erforderlich, anzupassen. Die erstellten Dokumentationen sind an den AG nach Beendigung der Tätigkeit zu übergeben.

Dienstleistung Nachhärten der GA-Komponenten: pauschal oder nach Stunden

4.5.4 Audit Trails für Nachverfolgung (Protokollierung)

Gemäß dem VDMA EB 24774 benötigen Gebäudeautomationssysteme im Nichtwohnbereich bei netzwerkfähigen Komponenten mit Benutzerverwaltung eine Protokollierung und Nachverfolgung von relevanten Systemereignissen und Benutzeraktivitäten.

Der Bieter muss sicherstellen, dass die mit dem AG abgestimmten relevanten Statusänderungen von GA- Komponenten, Benutzeraktivitäten sowie manuellen Werteänderungen protokolliert und optional kommentiert werden können. Die Protokollierungsdaten sollten an einer zentralen Stelle gespeichert werden. Es muss sichergestellt sein, dass die aufgezeichneten Protokollierungsdaten nicht verändert oder gelöscht werden können. Die Protokollierungsdaten müssen zur Auswertung verfügbar gemacht werden.

Eine Protokollierung von Benutzerdaten muss DSGVO konform erfolgen.

Dienstleistung Implementierung eines GA-Audit-Trails: pauschal oder nach Stunden

4.5.5 Arbeitsvorschriften/Verhaltensanweisungen

Gemäß dem VDMA-Einheitsblatt 24774, ist die Erstellung und Ausführung der Risikoanalyse durch qualifiziertes eigenes Personal oder durch einen qualifizierten Dienstleister durchzuführen. Die Qualifikation ist nachzuweisen.

Basierend auf der Risikoanalyse sind durch den Bieter Arbeitsvorschriften und Verhaltensanweisungen zum dauerhaften Erhalt der IT-Sicherheit der Gebäudeautomation zu erstellen, und dem Betreiber zur Abnahme zu übergeben.

Die organisatorischen Maßnahmen in diesem Objekt sind mit den benannten Verantwortlichen für OT- und IT-Sicherheit abzustimmen und an diese zu übergeben und in bauseits bereits existierende SOPs (Standard Operating Procedure) zu integrieren.

Die Arbeitsvorschriften und Verhaltensanweisungen (Standard Operating Procedure - SOP) müssen ab Beginn des Anlagebetriebs für den

- SOP-Normalbetrieb, welcher sicherstellt, dass alle Sicherheitselemente dauerhaft funktionsfähig sind und auf dem neuesten Stand gehalten werden.

- SOP-Störfall, welcher die Abläufe und Informationen für die Aufklärung eines Störfalls oder möglichen Angriffs mit Schadensbegrenzung und -bewältigung festlegt.

Die SOPs umfassen mindestens die Beschreibung der Arbeitsabläufe des SOP-Normalbetrieb und im SOP-Störfall.

Die Checklisten für den SOP-Störfall müssen mindestens alle Informationen über die einzuhaltenden Meldewege, Rufnummern, Eskalationsstufen, Sofortmaßnahmen enthalten.

Die Dokumente sind für die Abnahme der Anlage beizubringen.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.5.6 Engineering Software/Werkzeuge

Gemäß dem VDMA-Einheitsblatt 24774 hat der Bieter sicherzustellen, dass alle Arbeitsgeräte (z.B. mobile Datenträger, Installationsmedien, Notebooks) entsprechend dem Schutzbedarf für dieses Projekt verwendet werden.

Mindestens jedoch ist sicherzustellen, dass alle Arbeitsgeräte (z.B. mobile Datenträger, Installationsmedien, Notebooks) vor dem Einsatz auf bekannte Schadsoftware geprüft werden. Das Ergebnis ist zu dokumentieren.

Der Bieter hat sicherzustellen, dass bei allen Software Engineering Werkzeugen, die an die Gebäudeautomation angeschlossen werden, ein aktueller Malwareschutz installiert und aktiv ist, und alle empfohlenen Patches installiert sind. Sollte dies aus technischen Gründen nicht möglich sein, muss der Bieter gleichwertig geeignete Schutzmaßnahmen nachweisen und deren Installation, und Anwendung dokumentieren sein. Die Dokumentation ist beizubringen.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.5.7 Dokumentation

Gemäß dem VDMA-Einheitsblatt 24774 erstellt der Bieter die Dokumentation der sicherheitsrelevanten IT-Maßnahmen als SOP und übergibt diese dem Betreiber.

Der Bieter muss die verwendeten Komponenten, die aktvierten und deaktivierten physischen Kommunikationsschnittstellen, die Protokolle und Zugänge der Komponenten und die Zugriffsmöglichkeiten zur GA dokumentieren.

Der Bieter muss die verfügbaren und genutzten Sicherheitseigenschaften der verwendeten Protokolle dokumentieren.

Der Bieter muss alle Wechselwirkungen und Abhängigkeiten von GA-relevanten Komponenten sowie von TGA-Anlagen, die in GA-Systeme integriert oder mit GA-Systemen gekoppelt sind, dokumentieren.

Die Dokumentation muss regelmäßig und bei Änderungen innerhalb der GA geprüft und angepasst werden. Der Bieter hat die Fortführung und Revisionierung der Dokumentation durch den Betreiber zu ermöglichen.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.5.8 Betreiberinformation/-schulung (Schulung GA-Sicherheitsrichtlinien)

Gemäß dem VDMA EB 24774 hat der Bieter den Betreiber in der korrekten Bedienung der IT-Sicherheit der Gebäudeautomation zu schulen.

Dem Betreiber sind die potenziellen Risiken der errichtende Anlage bezüglich der IT-Sicherheit seiner Gebäudeautomation zu vermitteln und mögliche Gefahren aufzuzeigen.

Der Bieter erstellt ein Schulungskonzept, in dem die Abläufe, Anwendung der Checklisten, sowie der SOP-Normalbetrieb und der SOP-Störfall vermittelt wird. Die Durchführung der Schulung ist zu dokumentieren.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.5.9 Backup / Restore

Gemäß dem VDMA EB 24774 ist für die Gebäudeautomation ein Prozess für das Sichern und Wiederherstellen der GA-relevanten, gefährdeten IT-Komponenten zu definieren und zu dokumentieren.

Der Bieter muss die Sicherung der Konfiguration von Systemen sicherstellen, so dass ein Wiedereinspielen einer fehlerfreien Version möglich ist. Das Backup-Konzept muss die genutzten Softwarekomponenten und die projektspezifische Projektierung und Programmierung

der GA-Komponenten umfassen. Der Bieter stimmt die Verwendung einer vorhandenen Infrastruktur oder eine alternative projektspezifische Backup-and-Restore Lösung mit dem Betreiber ab.

Ein Notfallhandbuch für die Wiederanlauf- und Wiederherstellungsplanung ist in Anlehnung an BSI-Standard 200-4 zu erstellen.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

4.5.10 Abnahmetest

Gemäß dem VDMA-Einheitsblatt 24774 hat der Bieter vor der Inbetriebnahme eines Systems sicherzustellen, dass die Systeme gemäß den IT-Sicherheits-Vorgaben konfiguriert sind.

Der Bieter sollte hierfür Tests spezifizieren, mit denen die Konformität der Konfiguration mit den Vorgaben nachgewiesen wird. Dafür kann auf vorhandene Zertifizierungen der Hersteller oder Betreiber zurückgegriffen werden. Die Testdurchführung sollte in einem Testbericht dokumentiert werden. Abweichungen von den Vorgaben, die die Sicherheit reduzieren, sind zu beheben.

Dienstleistung Erfüllung der Leistungen gemäß Vortext: pauschal oder nach Stunden.

Kontakt:
Thomas Müller
Fachverband Automation + Management für Haus + Gebäude
Telefon: +49 69 6603-1636
E-Mail: Thomas.Mueller@VDMA.eu

Lobbyregister: R000802
EU-Transparenzregister ID: 9765362691-45

vdma.eu/AMG