Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein INF.13 Technisches Gebäudemanagement

1. Einleitung

Ein gut auf die Gegebenheiten des Gebäudes abgestimmtes und sicheres technisches Gebäudemanagement (TGM) ist wichtig, um die technische Gebäudeausrüstung (TGA) eines Gebäudes optimal zu betreiben, zu pflegen und weiterzuentwickeln.

Im Baustein INF.13 *Technisches Gebäudemanagement* und somit auch in diesen Umsetzungshinweisen wird der Begriff Gebäude synonym für Gebäude, Gebäudekomplex, Liegenschaft und Liegenschaftsportfolio genutzt. Die unterschiedlichen Gebäudetypen werden in Kapitel 1.2 definiert. Falls Aspekte für spezielle Gebäudetypen gelten, werden diese explizit genannt. Ein Problem im TGM ist die Gemengelage. Oft ist nicht ein einzelner Betreiber des TGM zu benennen, wenn unterschiedliche Gewerke verschiedene Betreiber haben. Hinzu kommen der Eigentümer des Gebäudes und gegebenenfalls auch noch Mieter oder andere Nachfrageorganisationen. Daher ist auch die maßgeblich für das TGM zuständige Haustechnik nicht zwingend genau einer der genannten Parteien zuzuschreiben. Die Haustechnik kann daher verschiedene Parteien in sich vereinen oder auch übergeordnet zwischen ihnen koordinieren.

1.1. Abgrenzung

Die Zusammenhänge und insbesondere die Abgrenzung zwischen TGA, TGM und Gebäudeautomation (GA) ist zum Verständnis des Bausteins INF.13 *Technisches Gebäudemanagement* und der zugehörigen Umsetzungshinweise wesentlich. Abbildung 1 gibt einen Überblick über diese Abgrenzung, indem TGA, TGM und GA in einem Gebäude, dargestellt als ein Haus, angeordnet werden.

Die TGA stellt wesentliche technische Funktionen eines Gebäudes bereit. Sie bildet sozusagen das Fundament des Gebäudes. Beispiele für TGA sind Stromanlagen, Heizungsanalagen, Lüftungsanlagen, Förderanlagen (z. B. Aufzug) und Beleuchtungsanlagen.

Die TGA wird durch das im Bild darüber befindliche TGM betrieben, gepflegt und weiterentwickelt. Im TGM können verschiedene Werkzeuge, z. B. Computer-Aided Facility Management (CAFM) und Building Information Modeling (BIM) genutzt werden.

Falls die TGA automatisiert und gewerkübergreifend betrieben werden soll, wird zusätzliche technische Infrastruktur zur GA eingesetzt. Somit ist die GA ein zentrales Werkzeug des TGM und deshalb im Bild wie die anderen Werkzeuge des TGM innerhalb des TGM angeordnet.

Ein Gebäude kann durch TGM auch ohne GA betrieben werden, GA hingegen ist immer durch TGM flankiert.

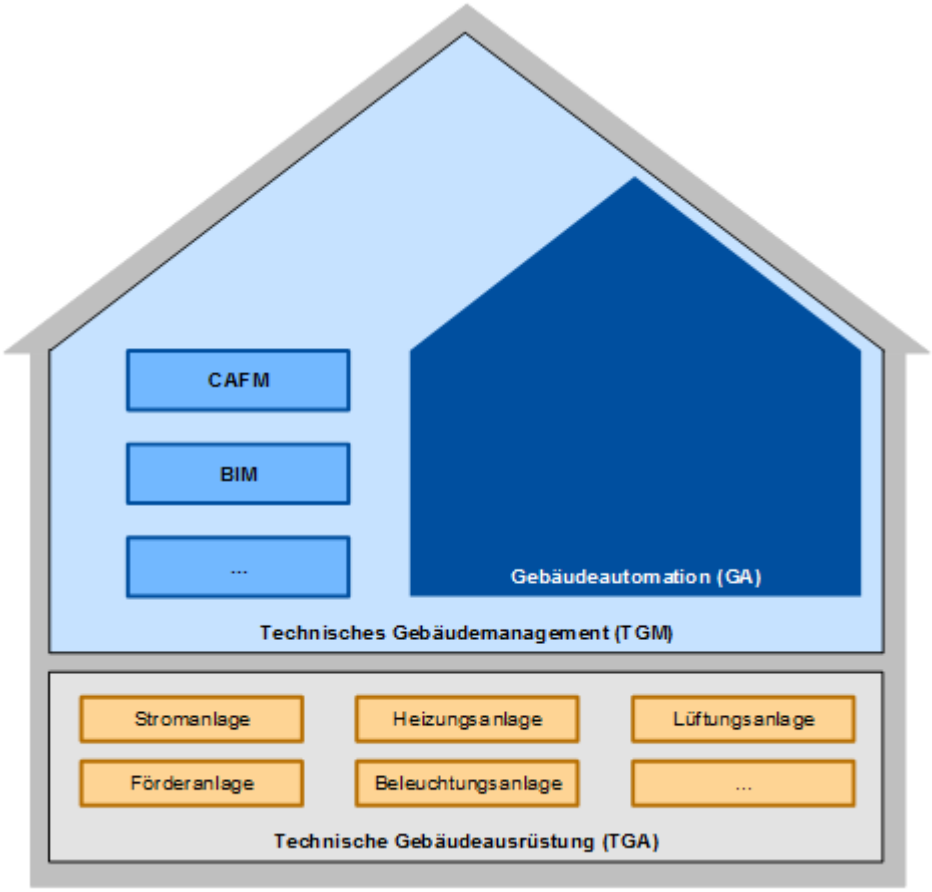

Abbildung 1: Abgrenzung TGM, GA und TGA-Anlagen

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins INF.13 *Technisches Gebäudemanagement* aufgeführt.

Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1. Maßnahmen zum Baustein INF.13 Technisches Gebäudemanagement

INF.13.M1 Beurteilung des Ist-Zustands bei der Übernahme bestehender Gebäude (B)

Werden bestehende Gebäude übernommen, ist es wichtig, sich zunächst einen Überblick über den Zustand der vorhandenen TGA und eines gegebenenfalls vorhandenen TGMs zu verschaffen. Dabei sollten direkt Informationen wie z. B. Hersteller, Versionsstand, Alter usw. für die Dokumentation erfasst bzw. überprüft werden (siehe INF.13.M3 *Dokumentation von Gebäudeeinrichtungen*). So können potenziell anstehende Reparaturen oder Modernisierungen sinnvoll geplant werden.

Bei der Prüfung muss sowohl für die TGA als auch für ein gegebenenfalls vorhandenes TGM beurteilt werden, ob die eingesetzten Systeme ausreichend sicher sind und weiter betrieben werden können. Dazu gehört z. B., dass sie keine bekannten signifikanten Schwachstellen aufweisen, angemessen gehärtet und sicher konfiguriert sind. Ist dies nicht der Fall, muss eine Strategie für den Umgang mit diesen Systemen entwickelt werden. Im Rahmen dieser Strategie sollte auch in Betracht gezogen werden, solche Systeme gegen neue Systeme zu ersetzen, sodass die Gefährdungen nur für eine begrenzte Zeit toleriert werden müssen, sofern keine Gegenmaßnahmen ergriffen werden können.

Außerdem muss für den Fall, dass bereits ein TGM vorhanden ist und weitergenutzt werden kann, überprüft werden, ob es TGA gibt, die nicht in das TGM eingebunden ist. Ziel ist es, möglichst alle TGA in das TGM einzubinden, damit die gesamte TGA optimal betrieben, gepflegt und weiterentwickelt werden kann. Dies gilt natürlich auch, wenn ein neues TGM aufgebaut und eingerichtet werden muss.

Neben den Systemen selbst darf auch die zugehörige Dokumentation nicht außer Acht gelassen werden. Es ist wichtig zu prüfen, ob die Bestandsdokumentation korrekt und vollständig ist und weiterverwendet werden kann oder erneuert bzw. aktualisiert werden muss. Häufig werden Änderungen oder Ergänzungen an Einrichtungen nicht in der Dokumentation nachgepflegt. Eine nicht aktuelle Dokumentation kann aber im Fall einer Störung unnötig Zeit kosten.

INF.13.M2 Regelung und Dokumentation von Verantwortlichkeiten und Zuständigkeiten im Gebäude (B)

Für jedes System bzw. jede zusammengehörige Systemgruppe, das bzw. die durch das TGM betreut wird, muss eindeutig festgelegt und dokumentiert sein, wer dafür verantwortlich und zuständig ist. Gegebenenfalls muss dies auch für einzelne Tätigkeiten unterschieden werden.

Dabei müssen Zuständigkeit und Verantwortlichkeit nicht in einer Hand liegen. Der Zuständige ist verpflichtet, dem Verantwortlichen regelmäßig und bei bestimmten Ereignissen Bericht zu erstatten. Nur so hat der Verantwortliche alle Informationen, um durchzuführende Handlungen zu verantworten oder bestehende Risiken zu übernehmen und gegebenenfalls steuernd eingreifen zu können. Gerade im Hinblick auf die Gemengelage zwischen Eigentümer, Mieter und gegebenenfalls Betreiberorganisationen müssen die Zuständigkeiten und Verantwortlichkeiten festgelegt und dokumentiert werden, um klare Verhältnisse zu schaffen.

Aufgrund der Gemengelage ist auch die Kenntnis der organisatorischen Strukturen im Gebäude wesentlich für die Abläufe des TGM. Die Konstellation in einem Gebäude kann einfach, aber auch sehr komplex sein. Gegebenenfalls sind mehrere Nachfrageorganisationen und Betreiberorganisationen beteiligt. Daher ist es wichtig zu klären, welche Parteien zu berücksichtigen sind. Im Folgenden werden zur Verdeutlichung beispielhaft eine einfache und eine komplexe Konstellation dargestellt.

Im einfachen Beispiel (siehe Abbildung 2) gibt es als Nachfrageorganisation nur den Eigentümer des Gebäudes. Er plant, nutzt und betreibt das Gebäude mit allen Infrastrukturen alleine. Damit ist er nicht nur Nachfrageorganisation, sondern auch zuständig für die Planung und den Betrieb. Der Eigentümer ist also hier in der Rolle der Betreiberorganisation für TGM und Gebäudeautomation (GA). Für bestimmte TGA, beispielsweise für die Aufzugsanlange, setzt er separate TGA-Betreiberorganisationen ein.

Der Eigentümer ist in diesem Fall der Gebäudeverantwortliche und trägt die Gesamtverantwortung.

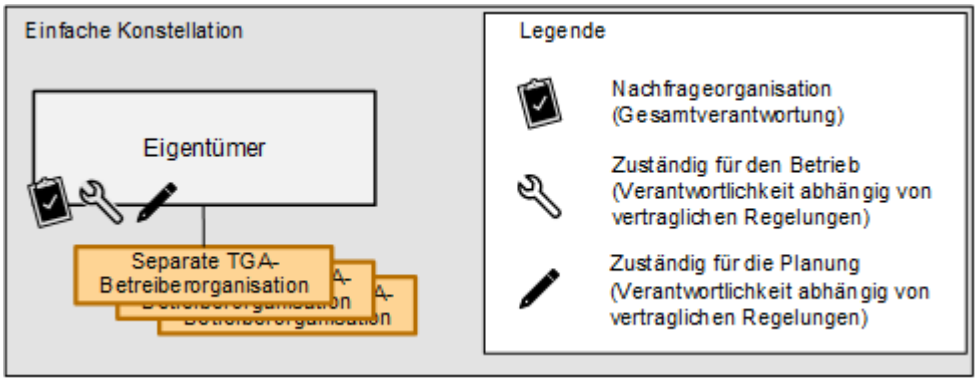

Abbildung 2: Einfache Konstellation der organisatorischen Strukturen im Gebäude

Im zweiten Beispiel (siehe Abbildung 3) setzt der Eigentümer des Gebäudes eine Verwaltungsorganisation zur Verwaltung und Organisation der Mieter und der Betreiberorganisation A des Gebäudes ein.

Betreiberorganisation A ist für den Betrieb der gemeinsam genutzten Gebäudeinfrastruktur (also auch für das TGM dieser Gebäudeinfrastruktur) zuständig und setzt eine separate Betreiberorganisation B für die GA sowie separate TGA-Betreiberorganisationen ein, z. B. für den Aufzug. Betreiberorganisation B für die GA setzt wiederum separate TGA-Betreiberorganisationen für ihren Bereich ein.

Während der Planungs- und Ausführungsphase setzt der Eigentümer einen Generalunternehmer (GU) ein, der in dieser Phase für die Planung und Ausführung zuständig ist. Nach Abschluss der Planungs- und Ausführungsphase übernimmt der Eigentümer weitere Planungen selbst oder übergibt sie ganz oder teilweise der Verwaltungsorganisation.

Mieter 1 hat keine eigene Gebäudeinfrastruktur. Anforderungen an die gemeinsam genutzte Gebäudeinfrastruktur richtet er an die Verwaltungsorganisation. Er ist weder für die Planung noch für den Betrieb einer Gebäudeinfrastruktur zuständig.

Mieter 2 hat zum Teil eigene Gebäudeinfrastruktur, wie Beleuchtung, Überwachung der Belegung der Besprechungsräume, Luminous Carpet und Indoor-Navigation. Für den Betrieb dieser eigenen Gebäudeinfrastruktur, inklusive entsprechendem TGM und GA, ist Betreiberorganisation C zuständig. Diese setzt selbst separate TGA-Betreiberorganisationen ein. Mieter 2 ist für die Planung für die eigenen Gebäudeinfrastrukturen zuständig.

Mieter 3 hat ebenfalls zum Teil eigene Gebäudeinfrastrukturen. Er betreibt sein TGM und seine GA selbst, setzt aber separate TGA-Betreiberorganisationen ein. Er ist also sowohl für die Planung als auch für den Betrieb seiner eigenen Gebäudeinfrastrukturen zuständig.

Außerdem lässt Mieter 3 einen Dienstleister (als Untermieter) die Kantine betreiben. Dieser setzt für den Betrieb seiner eigenen Gebäudeinfrastruktur wiederum eine Betreiberorganisation D ein (TGM und GA). Die Kantine ist für die Planung ihrer eigenen Gebäudeinfrastruktur zuständig.

In dieser Konstellation ist der Eigentümer der Gebäudeverantwortliche. Er kann die Verantwortung z. B. für Schneeräumung, Internetversorgung, Zutrittsregelung, Stromversorgung, TGA etc. an Dritte übergeben, hier die Verwaltungsorganisation oder Mieter.

Nachfrageorganisationen sind in diesem Beispiel der Eigentümer, die Verwaltungsorganisation und die Mieter inklusive Untermieter, d. h. die Kantine von Mieter 3.

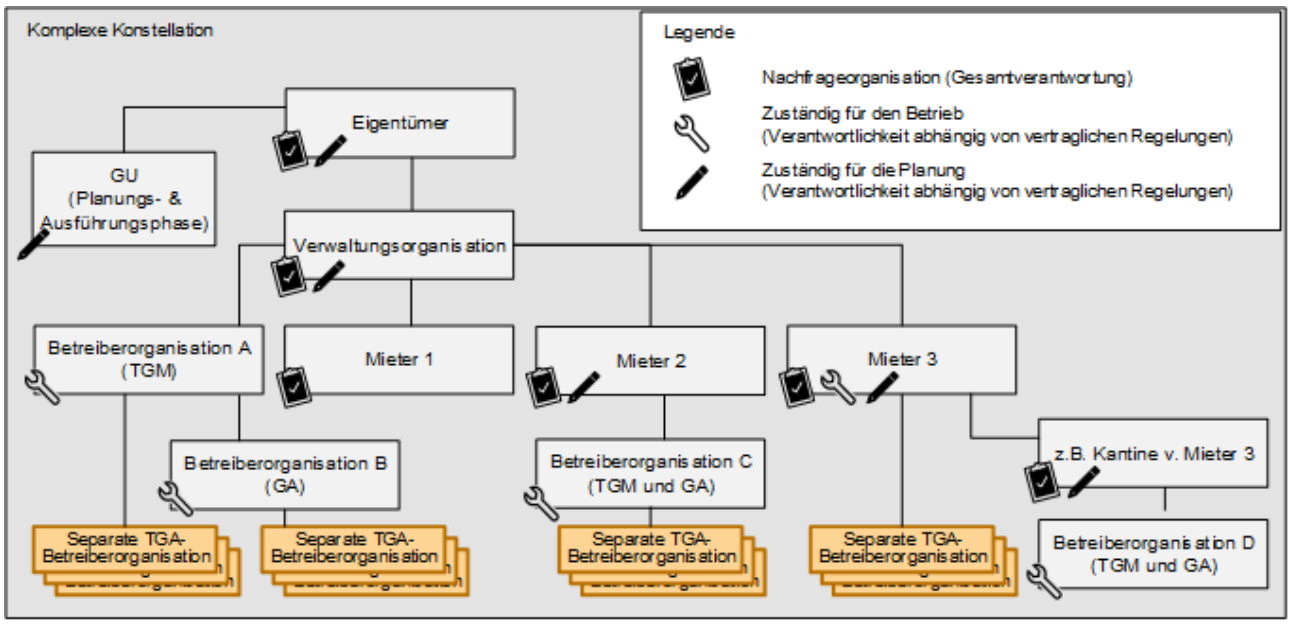

Abbildung 3: Komplexe Konstellation der organisatorischen Strukturen im Gebäude

Gerade in komplexen Konstellationen ist es wichtig, alle Nachfrage- und Betreiberorganisationen zu erfassen. Sämtliche Zuständigkeiten und Verantwortlichkeiten sowie Rechte, Pflichten, Aufgaben und Kompetenzen und die zugehörigen Prozesse müssen eindeutig dokumentiert werden. Dies hilft auch für den Fall, dass eine Betreiberorganisation gewechselt werden soll.

Auch Zuständigkeiten innerhalb einer Institution können hier von Belang sein. Werden beispielsweise von IT und TGA gemeinsame Netze und gegebenenfalls auch gemeinsame Plattformen genutzt, sollte geklärt und dokumentiert werden, wer für welche Belange zuständig ist und wo Schnittstellen bestehen. Dies ist wichtig, damit diese Zuständigkeitsdiskussionen nicht erst im Fall einer Störung geführt werden und dann kostbare Zeit verloren geht, die besser für die Fehlersuche und -behebung verwendet werden kann.

Zu den Prozessen, die im Zusammenhang mit den Aufgaben und Pflichten dokumentiert werden müssen, gehören auch Regelungen darüber,

- welche physischen Zugänge oder Fernzugänge für die Durchführung der Aufgaben benötigt werden,
- welche Meldewege genutzt werden müssen, z. B. E-Mail, Ticket-System etc. und
- welche Eskalationsstufen wann eingeleitet werden müssen.

Außerdem muss klar dokumentiert sein, wer im Fehler- bzw. Störungsfall informiert werden muss, damit weitere Schritte gemäß dem festgelegten Eskalationsprozess eingeleitet werden können. Hierbei müssen auch Vertretungsregeln berücksichtigt werden.

Auch die Schnittstelle zu externen Dritten, die gegebenenfalls für Reparatur und Wartung zuständig sind und im Fehler- bzw. Störungsfall hinzugezogen werden, muss festgelegt und dokumentiert werden.

Die zugehörige Dokumentation muss aktualisiert werden, sobald sich Zuständigkeiten, Verantwortlichkeiten, Pflichten, Aufgaben oder Prozesse ändern. Außerdem sollte sie zusätzlich regelmäßig überprüft und gegebenenfalls angepasst werden. Da die Dokumentation vertrauliche Daten enthält, muss der Zugriff darauf entsprechend der allgemeinen Regeln des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* abgesichert werden.

INF.13.M3 Dokumentation von Gebäudeeinrichtungen (B)

Die Dokumentation von Gebäudeeinrichtungen umfasst alle Informationen, die zur Nutzung, zum Betrieb und zur Instandhaltung dieser Einrichtungen notwendig sind. Das TGM ist auf eine

vollständige und stets aktuelle Dokumentation angewiesen, bei der alle Daten und Pläne eines Gebäudes geordnet und gut lesbar an geeigneter zentraler Stelle zur Verfügung stehen.

Große Teile der Dokumentation werden bereits beim Bau eines Gebäudes erstellt. Hierfür gibt es z. B. eine Dokumentationsrichtlinie des Bundesamts für Bauwesen und Raumordnung (BBR). Diese legt fest, wie Grundrisspläne angefertigt werden, die für jeden Raum alle Informationen beinhalten, die für den Bau und für die Installationen während des Baus wichtig sind. Ausführende und Errichter von TGA-Anlagen erstellen Bestandslisten. Technische Dokumentation von installierten Einrichtungen wird übergeben. Diese gesamte Dokumentation muss zusammengeführt und vor allem nach neuen Gesichtspunkten geordnet und organisiert werden. Es ist wichtig, dass eine TGM-gerechte Nutzungsdokumentation entsteht, die eine nutzungsorientierte Systematik nach TGM-Kriterien aufweist.

Zu bedenken ist auch, dass beim Bau eines Gebäudes oft gänzlich andere Personen beteiligt sind als anschließend im TGM. Bei diesem Personenwechsel dürfen keine Informationen aufgrund unzureichender Schnittstellen verloren gehen. Manchmal ist die Ist-Dokumentation nach Bau-Fertigstellung unvollständig und unzureichend. Auch wenn das Erbringen entsprechender Unterlagen in der Regel durch Vorschriften vorgeschrieben ist, zeigt die Praxis, dass die Ist-Dokumentation nicht immer vollständig eingefordert wird und somit nicht zwingend vollständig vorliegt. Bei einem Neubau muss daher darauf geachtet werden, dass die Dokumentation vollständig vorliegt und dem TGM zur Verfügung gestellt wird. Ist die Dokumentation bei späterer Übernahme eines Gebäudes unvollständig, muss versucht werden, über den Vorbesitzer bzw. Vorbetreiber oder die entsprechenden Installationsfirmen fehlende Dokumentation zu erhalten. Gegebenenfalls muss eine Nachdokumentation erstellt werden (siehe auch INF.13.M1 *Beurteilung des Ist-Zustands bei der Übernahme bestehender Gebäude*).

Eine TGM-gerechte Nutzungsdokumentation geht von einer Übersicht aus, die zeigt, für welche Gebäudeeinrichtungen das TGM zuständig ist. Für jede Einrichtung müssen weitere für das TGM erforderliche und wichtige Informationen vorhanden sein. Zu den zu erfassenden Einrichtungen gehören mindestens:

- Stromleitungen inkl. Unterbrechungsfreier Stromversorgungen (USV) und Netzersatzanlagen (NEA)
- Kommunikationsleitungen inkl. Steuerleitungen
- Blitzschutzeinrichtungen
- Entwässerungseinrichtungen
- Gefahrenmeldeanlagen
- Klimatisierungsanlagen und raumlufttechnische Anlagen (RLT-Anlagen)
- Zutrittskontrollsysteme
- Förderanlagen
- Videoüberwachungssysteme
- Technische Ausstattung der Gebäudeautomation

Pro Einrichtung müssen Ausrüstungs- und Inventarverzeichnisse vorhanden sein sowie Informationen für Betrieb, Wartung und Pflege der Einrichtungen. Hierzu gehören z. B. Informationen darüber,

- was alles zu der Einrichtung gehört (z. B. Sensoren, Aktoren, Beacons), jeweils mit
    - Hersteller,
    - Systemstand von Hardware und Software,
    - Ausstattung und Alter,
    - Kommunikationsschnittstellen,

    - Zugriffsmöglichkeiten und
    - gegebenenfalls sonstige spezielle Anforderungen, wie z. B. 24x7-Verfügbarkeit,
- wo sich die zugehörigen Systeme und Komponenten befinden,
- welche regelmäßigen Arbeiten in welchen Intervallen erledigt werden müssen,
- wer benachrichtigt werden muss, wenn etwas nicht funktioniert und
- welche Rückwirkungen auf andere Systeme es gibt.

Die gesamte Dokumentation muss stetig aktuell gehalten werden, indem sämtliche Änderungen nachgepflegt werden. Außerdem sollte sie regelmäßig überprüft und gegebenenfalls angepasst werden. Da die Dokumentation vertrauliche Daten enthält, muss der Zugriff darauf entsprechend der allgemeinen Regeln des Bausteins ORP.4 *Identitäts- und Berechtigungsmanagement* abgesichert werden.

INF.13.M4 Erstellung einer Sicherheitsrichtlinie für TGM (S)

Die zu erstellende Sicherheitsrichtlinie legt die Rahmenbedingungen und allgemeine Vorgaben zur Ausgestaltung der Themen in den Konzepten fest, d. h. ihr Detaillierungsgrad ist weniger tief als der eines Konzepts. Allerdings hat sie Weisungscharakter und muss ebenso wie ihre Aktualisierungen allen Personen, die am TGM beteiligt sind, bekanntgemacht werden. Dies ist wichtig, um die Administratoren für die getroffenen Sicherheitsvorschriften zu sensibilisieren (siehe auch Baustein ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*). Gerade Administratoren mit privilegierten Rechten und die Managementkommunikation mit für Angreifer relevanten Inhalten bilden ein erhebliches Angriffsziel. Daher ist es wichtig, die Umsetzung der Inhalte der Sicherheitsrichtlinie regelmäßig nachvollziehbar zu prüfen und zu aktualisieren. Hierfür können z. B. Soll-Ist-Vergleiche herangezogen werden. Außerdem sollte der Stand der Technik in regelmäßigen Aktualisierungen der Sicherheitsrichtlinie einfließen.

Die Sicherheitsrichtlinie für das TGM dokumentiert die wesentlichen Anforderungen und Bedingungen, die für das TGM berücksichtigt werden müssen. Die Sicherheitsrichtlinie sollte folgende Themenbereiche enthalten:

- Vorgaben, welche Bereiche des TGM über zentrale Werkzeuge und Dienste realisiert werden
  Es wird empfohlen, möglichst viele Bereiche des TGM über zentrale Werkzeuge und Dienste zu realisieren. Dies liegt darin begründet, dass zentrale Lösungen leichter abzusichern sind als eine Vielzahl dezentraler Lösungen.
- Vorgaben, inwieweit Aufgaben im TGM automatisiert realisiert werden sollen
  Aufgaben, die sinnvoll automatisiert werden können, sollten automatisiert realisiert werden. Hierzu gehört z. B. die automatisierte Verteilung von freigegebenen und getesteten Software-Updates und Konfigurationen an Systeme, die in das TGM eingebunden sind.
- Vorgaben für eingesetzte Werkzeuge
  Zunächst sollten allgemeine Vorgaben für alle für das TGM eingesetzten Werkzeuge bzw. Systeme spezifiziert werden. Gegebenenfalls gibt es darüber hinaus spezielle Vorgaben für eingesetzte Werkzeuge oder bestimmte Werkzeuge dürfen nicht eingesetzt werden.
- Vorgaben zur Zutritts-, Zugangs- und Zugriffskontrolle
  Zentrale TGM-Lösungen und die ihnen zugrundeliegende Infrastruktur, z. B. Virtualisierungslösungen, sollten sich grundsätzlich in physisch geschützten Bereichen befinden. Zugangs- und Zugriffsrechte sollten nach dem Minimalprinzip vergeben werden und den allgemeinen Richtlinien der Institution folgen. Der Zugang zu Systemen und der Zugriff auf Informationen darf nur nach erfolgreicher Authentisierung erlaubt werden (siehe auch Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*). Spezielle Regelungen zur Authentisierung sollten festgehalten werden. Zugang und Zugriff sollten grundsätzlich auf personengebundene Konten beschränkt werden.

- Vorgaben zum Schutz der Kommunikation
  Die TGM-Kommunikation sollte über sichere Protokolle erfolgen. Zumindest wenn über nicht vertrauenswürdige Netzsegmente kommuniziert wird, sollte die TGM-Kommunikation verschlüsselt werden.
- Operative Grundregeln
  Essentielle Grundregeln, die für den Betrieb und die Nutzung des TGM gelten, sollten in der Sicherheitsrichtlinie festgehalten werden. Hierzu sollte z. B. gehören, dass administrative Rechte für normale Nutzerkonten grundsätzlich zu vermeiden sind. Außerdem sollten administrative Konten ausschließliche für administrative Zwecke genutzt werden dürfen, damit diese mit privilegierten Rechten ausgestatteten Konten nicht bei normalen Nutzertätigkeiten kompromittiert werden können.
- Vorgaben zum Monitoring
  Die TGM-Lösungen sollten in ein zentrales Monitoring eingebunden werden.
- Vorgaben zur Protokollierung
  Die TGM-Lösungen sollten in eine zentrale Protokollierung eingebunden werden.

INF.13.M5 Planung des TGM (S)

Eine konsequente, detaillierte Planung des TGM sichert die optimale Nutzung der Gebäudeeinrichtungen und macht das TGM zu einem umfassenden Werkzeug zur Betrachtung, Analyse und Optimierung aller Vorgänge und Prozesse für die zu betreibende TGA.

Die Planung des TGM sollte mindestens eine detaillierte Anforderungsanalyse, eine ausreichende Grobkonzeptionierung und eine Fein- und Umsetzungsplanung umfassen. Dabei sollten alle in der Sicherheitsrichtlinie für TGM genannten Punkte berücksichtigt werden.

Detaillierte Festlegung der Anforderungen

In der Anforderungsanalyse für das TGM werden organisatorische und technische Anforderungen an die gesamte TGM-Infrastruktur festgehalten. Dies ist sowohl für die Konzeptionierung des TGM als auch für den Beschaffungsprozess von Lösungen für das TGM und für einzubindende Systeme wichtig.

Für TGM-Werkzeuge sollten mindestens Vorgaben für zu unterstützende und wünschenswerte Funktionen sowie Vorgaben für die Erweiterbarkeit der Werkzeuge spezifiziert werden. Außerdem sollten die Zugriffsmöglichkeiten auf die TGM-Systeme festgelegt werden, also welchen IT-Systemen der Zugriff auf die TGM-Systeme erlaubt werden soll und welche Protokolle dafür genutzt werden sollen. Die Zugriffsmöglichkeiten auf die TGM-Systeme sollten entsprechend eingeschränkt werden. Im Rahmen des Notfallmanagements werden für Notbetriebsformen gegebenenfalls weitere Zugriffsmöglichkeiten erlaubt.

Weiterhin sollten für das TGM nur sichere Protokolle mit aktivierten Sicherheits-Funktionen eingesetzt werden. Hierzu gehören nach dem Stand der Technik sichere Verschlüsselung, Authentisierung, Autorisierung und Integritätsschutz, die je nach Schutzbedarf der Daten und der Vertrauenswürdigkeit der Umgebung angewandt werden sollten. Entsprechend konkret zu unterstützende Protokolle sollten sowohl für TGM-Systeme als auch für die eingebundene TGA vorgegeben werden.

Für alle Systeme, die über das TGM verwaltet werden sollen, sollten zu erfüllende Vorgaben erfasst werden. Außerdem kann es auch Anforderungen an die TGM-Werkzeuge geben, die durch bestehende TGA vorgegeben werden. Werden alle Anforderungen an die zu verwaltenden Systeme in einem Lastenheft für das TGM erfasst und gewichtet, kann darauf bei jeder Beschaffung zurückgegriffen werden. So können übereilte, nicht durchdachte Aufträge verhindert werden, die Konsequenzen zum Beispiel bei der Kompatibilität zu bereits vorhandenen Produkten nach sich ziehen können. Insbesondere wenn auch Gebäudeautomation (GA) eingesetzt wird, sollten die diesbezüglichen Vorgaben und Anforderungen in einem GA-Lastenheft zusammengestellt werden.

Außerdem sollten gegebenenfalls bestehende Anforderungen an Schnittstellen zu Alarmierungssystemen, z. B. Lösungen für eine Alarmierung per E-Mail oder SMS, zu übergeordneten

Systemen eines Leitstands oder Helpdesks oder zu sonstigen übergreifenden Lösungen sowie zu einer zentralen Protokollierung und zu einem Security Information and Event Management (SIEM, siehe auch INF.13.M29 *Integration des TGM in ein SIEM*) spezifiziert werden.

Grobkonzeptionierung

Für die Grobkonzeptionierung sollte ein TGM-Konzept erstellt werden (siehe INF.13.M6 *Erstellung eines TGM-Konzepts*).

Fein- und Umsetzungsplanung

Die Feinplanung detailliert und konkretisiert die Grobkonzeptionierung des TGM. Dabei werden alle Punkte des TGM-Konzepts erneut aufgegriffen. Beispielsweise werden konkrete Konfigurationsvorgaben für die Management-Systeme und -Werkzeuge spezifiziert und gegebenenfalls spezielle Sichten bzw. Menüs innerhalb der Werkzeuge für unterschiedliche Nutzergruppen des TGM erstellt. Außerdem werden hier auch Tests und Abnahmetests spezifiziert, die für die Inbetriebnahme von Lösungen erforderlich sind. Weiterhin sollte festgelegt werden, für welche Systeme Autoupdates durchgeführt werden sollen.

In der Umsetzungsplanung wird festgelegt, wie das Feinkonzept umgesetzt werden soll. Die einzelnen notwendigen Schritte werden definiert. Ihre Reihenfolge, Zuständigkeiten und ein Zeitrahmen werden festgelegt.

Darüber hinaus sollte bereits bei der Planung daran gedacht werden, dass gerade bei einer 24x7-Verfügbarkeit nicht immer geschultes Personal für akut anfallende Arbeiten vor Ort ist. Daher ist es wichtig, die entsprechenden Prozesse und Arbeiten an die Qualifizierung der entsprechenden Mitarbeiter vor Ort anzupassen bzw. im Umkehrschluss die entsprechenden Mitarbeiter dahingehend zu schulen, dass sie diese anfallenden Arbeiten ausführen können.

Außerdem sollte bereits bei der Planung geprüft werden, ob im TGM Cloud-Dienste eingesetzt werden. Ist dies der Fall, sollte auch bedacht werden, ob und wie gegebenenfalls der Cloud-Dienstleister gewechselt werden kann. Unter Umständen ist die Abhängigkeit vom Cloud-Dienstleister so groß, dass bei einem Wechsel sogar neue TGA beschafft werden muss.

INF.13.M6 Erstellung eines TGM-Konzepts (S)

Das TGM-Konzept stellt eine Grobkonzeptionierung des TGM dar. Für alle Bereiche werden grundlegende Festlegungen getroffen. Dabei werden die Themen der Sicherheitsrichtlinie, der Planung und der Anforderungsspezifikation wieder aufgegriffen. Damit fasst das TGM-Konzept alle Aufgaben und Vorgaben im TGM zusammen und ist somit auch bei einem Wechsel der Betreiberorganisation von Bedeutung.

Das TGM-Konzept sollte regelmäßig und auch 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 ein Soll-Ist-Vergleich zwischen den Vorgaben des Konzepts und dem aktuellen Zustand durchgeführt werden, um unerlaubte Abweichungen vom Konzept aufzudecken, aber auch um gegebenenfalls notwendige Aktualisierungen des Konzepts erkennen zu können.

Weiterhin sollte das TGM-Konzept Verweise auf Aufbewahrungsorte wichtiger Unterlagen enthalten.

Methoden, Techniken und Werkzeuge für das TGM

Um Methoden, Techniken und Werkzeuge für das TGM zu spezifizieren, müssen zunächst grundlegende Festlegungen getroffen werden.

- Sollen das TGM oder Teile des TGM beispielsweise von externen Dienstleistern erbracht werden, sollte der Baustein 2.1 *Outsourcing für Kunden* berücksichtigt werden. Außerdem dürfen solche Outsourcing-Maßnahmen das Sicherheitsniveau nicht schwächen.
- Sollen für das TGM Cloud-Dienste genutzt werden, sollten der Baustein 2.2 *Cloud-Nutzung* sowie INF.13.M24 *Sicherstellung der Kontrolle über die Prozesse bei Cloud-Nutzung für das TGM*

und bei erhöhtem Schutzbedarf auch INF.13.M27 *Einrichtung einer Private Cloud für das TGM* berücksichtigt werden. Auch hier darf das Sicherheitsniveau nicht geschwächt werden.

Weiterhin sollte festgelegt werden, welche Werkzeuge im TGM eingesetzt werden sollen. Hierzu gehören auch generelle Entscheidungen über den Einsatz von Computer-Aided Facility Management (CAFM) und Building Information Modeling (BIM). Regelungen für den Einsatz dieser Werkzeuge finden sich in INF.13.M9 *Regelung des Einsatzes von Computer-Aided Facility Management* und INF.13.M10 *Regelung des Einsatzes von Building Information Modeling*. Insgesamt besteht das TGM meist aus verschiedensten Systemen und Elementen. Es sollte jedoch versucht werden, möglichst einheitliche zentrale Lösungen zu finden und einheitliche Regelungen zu definieren, um die Prozesse zu erleichtern und auch den Anpassungs-Aufwand bei möglichen Änderungen weitestgehend gering zu halten.

Außerdem muss die zu betreibende TGA betrachtet werden. Hier sollte festgelegt werden, welche TGA-Systeme über welches TGM-Werkzeug verwaltet werden und welche Protokolle dafür genutzt werden dürfen. In diesem Zuge sollten möglichst alle TGA-Systeme im TGM-Konzept behandelt werden, sodass der Umgang mit den Systemen, sowie aktuelle Regelungen definiert sind.

Absicherung des Zugangs und der Kommunikation

Jeglicher Zugriff auf das TGM sollte entkoppelt erfolgen. Außerdem sollten nur dedizierte Management-Clients verwendet werden, die nicht für andere Tätigkeiten genutzt werden.

Es sollten nur sichere Protokolle mit aktivierten Sicherheitsfunktionen eingesetzt werden, die die Kommunikation nach dem Stand der Technik sicher verschlüsseln und eine angemessene Authentisierung bieten. Die Zugriffsmöglichkeiten auf die TGM-Systeme sollten entsprechend eingeschränkt und die Kommunikation für das TGM abgesichert werden.

Außerdem sollte für das TGM ein Rollen- und Berechtigungskonzept erstellt, umgesetzt und gepflegt werden, das die speziellen Tätigkeiten und den zugehörigen Zugriff auf Informationen im TGM abbildet (siehe auch INF.13.M14 *Berücksichtigung spezieller Rollen und Berechtigungen im TGM*).

Absicherung auf Ebene des Netzes, insbesondere Zuordnung von TGM-Komponenten zu Netzsegmenten

Auf Ebene des Netzes wird durch den Baustein NET.1.1 *Netzarchitektur und -design* eine Netzsegmentierung gefordert. Für Ports an Access Switches sollte zur weiteren Absicherung eine Netzzugangskontrolle (Network Access Control, NAC) realisiert werden.

Bei der Zuordnung von TGM-Komponenten zu Netzsegmenten sollte die organisatorische Struktur im Gebäude berücksichtigt werden. Systeme unterschiedlicher Nachfrageorganisationen sollten z. B. in unterschiedlichen Netzsegmenten positioniert werden. Ebenso können Sicherheitskriterien und Schutzbedarf für eine Zuordnung von TGM-Komponenten zu Netzsegmenten herangezogen werden.

Umfang des Monitorings und der Alarmierung

Für jeden Systemtyp sollte festgelegt werden, welche Parameter im Monitoring überwacht werden und an wen bei Überschreitung von Schwellwerten eine Alarmierung erfolgen sollte (siehe auch INF.13.M19 *Konzeptionierung und Durchführung des Monitorings im TGM*).

Protokollierung von Ereignissen und administrativen Zugriffen

Ebenso sollte für jeden Systemtyp der Umfang der Protokollierung festgelegt werden (siehe auch INF.13.M21 *Protokollierung im TGM*).

Meldeketten bei Störungen und Sicherheitsvorfällen

Für Störungen und Sicherheitsvorfälle, die im TGM auftreten können, sollten Prozesse definiert werden, die das weitere Vorgehen und die Reaktion auf entsprechende Alarme spezifizieren. Um die entsprechenden Vorgänge auszulösen, sollten Meldeketten festgelegt werden, also wer wann und wie benachrichtigt werden muss. Zumindest die erste Alarmierung bei einem durch das Monitoring erkannten Vorfall sollte automatisiert erfolgen. Hier ist neben einer einfachen Alarmmeldung auf einer

Managementstation eine Weiterleitung von Alarmen zu übergreifenden Werkzeugen im Leitstand sowie eine Meldung per E-Mail, SMS oder über Pager denkbar.

Benötigte Prozesse für das TGM

Die für das TGM benötigten Prozesse sollten mit Zuständigkeiten und Übergabepunkten definiert werden. Hierzu gehören mindestens

- Prozesse für die Verarbeitung von Informationen bzw. Daten (Sammlung, Zusammenfassung, Aufbewahrung, Sicherheit)
- Prozesse für Änderungen im TGM (siehe auch 13.M16 *Prozess für Änderungen im TGM*)
- Prozesse für Störungen inklusive Störfall-, Meldungs- und Informationsmanagement sowie Eskalationswegen und -zeiten
- Prozesse für Wartung und Pflege der Systeme (siehe auch 13.M17 *Regelung von Wartungs- und Reparaturarbeiten im TGM* und INF.13.M18 *Proaktive Instandhaltung im TGM*
- Verweise auf Aufbewahrungsorte wichtiger Unterlagen bzw. Quell-Dokumente

Bereitstellung von TGM-Informationen für andere Betriebsbereiche

Werden Informationen aus dem TGM für andere Betriebsbereiche benötigt, z. B. Protokollierungsdaten für ein übergreifendes Security Monitoring, sollte festgelegt werden, wie und zu welchen Zeitpunkten diese Daten bereitgestellt werden sollen und über welche Schnittstellen sie übermittelt werden.

Einbindung des TGM in die Notfallplanung

Das TGM sollte in das Notfallhandbuch gemäß Baustein DER.4 *Notfallmanagement* aufgenommen und somit in Wiederanlauf- und Wiederherstellungspläne integriert werden. Hierbei sollten Prioritäten von Gebäude und Systemen berücksichtigt werden. Ansprechpartner für die Systeme des TGM sollten bei den Verantwortlichen für das Notfallmanagement hinterlegt werden. Außerdem sollten für alle TGM-Lösungen regelmäßige Datensicherungen erfolgen, um eine schnelle Wiederherstellung der Systeme zu ermöglichen.

Für den Fall, dass nicht die TGM-Lösung selbst ausfällt, sondern nur der Zugang zu dieser, sollten gegebenenfalls zusätzliche Zugangswege zur TGM-Lösung spezifiziert werden, die nur in diesem Fall freigeschaltet werden. Hier ist beispielsweise ein redundanter Internetanschluss geringerer Bandbreite möglich, z. B. ein vDSL-Anschluss kombiniert mit einem VPN zur Absicherung der Kommunikation. Auch ein Zugang über 5G oder eine ältere Mobilfunktechnik wie LTE ist möglich. Dieser sollte dann aber nur aktiviert werden, wenn er benötigt wird. Die Aktivierung sollte nachvollziehbar begründet und autorisiert werden und nach Beendigung des Notfalls wieder deaktiviert werden. Auch die Festlegung von Notbetriebsformen ist denkbar.

INF.13.M7 Erstellung eines Funkfrequenzkatasters (S)

Ein Funkfrequenzkataster ist eine Übersicht aller genutzten Funkfrequenzen. Dabei werden sämtliche Funkfrequenzen der eingesetzten Funksysteme von WLAN und Mobilfunk über Bluetooth bis zur Mikrowelle berücksichtigt. Wenn Frequenzbereiche von unterschiedlichen Funksystemen gemeinsam verwendet werden, sind grundsätzlich Interferenzen nicht ausgeschlossen. Daher sollte für die verschiedenen Frequenzen ein Primärnutzer festgelegt werden.

Typische Felder in einem Funkfrequenzkataster sind:

- Bezeichnung des Funksystems
- Frequenzbereiche
- Kanäle
- Sendeleistung Basisstation und Mobilgeräte
- Antennentypen

- Übertragungsverfahren
- Typischer Einsatzort
- Ansprechpartner

Anhand dieser Auflistungen lassen sich Störungen im Vorfeld vorhersehen bzw. Fehler im tatsächlichen Störungsfall schneller finden.

Wichtig ist, dass immer das Gesamtbild betrachtet wird. Daher sollten hier auch Funksysteme erfasst werden, die nicht zum TGM gehören, aber in Bereichen genutzt werden, in denen auch Funksysteme eingesetzt werden, die zum TGM gehören. Beispiele sind WLAN-Systeme der IT, Funksysteme der OT und Systeme des BOS-Funk im Fall von Behörden und Organisationen mit Sicherheitsaufgaben. Außerdem können nicht nur Störungen von Systemen innerhalb des Gebäudes zu Beeinträchtigungen oder Ausfällen führen, sondern auch starke Funksignale im nahen Umfeld des Gebäudes, die in das Gebäude hereinstrahlen. Ein Beispiel bilden hier Bahntrassen mit regelmäßigem Verkehr.

Im Idealfall kann schon vor Einsatz der verschiedenen Funkfrequenzen, beispielsweise bei einem Neubau, eine entsprechende Risikoanalyse erfolgen, die darstellt mit welchen Beeinträchtigungen zu rechnen ist.

INF.13.M8 Erstellung und Pflege eines Inventars für das TGM (S)

In ein Inventar sollten sämtliche Systeme und damit verbundenen Elemente aufgenommen werden, die durch das TGM verwaltet werden. Wird ein Computer-Aided Facility Management-System (CAFM-System) eingesetzt, kann das Inventar gegebenenfalls darin integriert werden (siehe auch INF.13.M9 *Regelung des Einsatzes von Computer-Aided Facility Management*).

Für jedes System sollten mindestens folgende Daten erfasst werden:

- Hersteller
- Systemstand von Hardware und Software
- Ausstattung und Alter
- Kommunikationsschnittstellen
- Zugriffsmöglichkeiten
- Wartungszyklen
- Zuständige und Verantwortliche

Wünschenswert ist weiterhin pro System der Verweis auf dessen Konfiguration und auch auf Wartungsverträge oder sonstige Verträge. Auf diese Weise werden alle wichtigen Informationen über ein System an einer Stelle zugänglich gemacht.

Ein Inventar ist nicht nur aus einem betrieblichen und kaufmännischen Blickwinkel wichtig, indem es Informationen sinnvoll zusammenstellt und damit Prozesse vereinfacht. Es ist auch für die Informationssicherheit wesentlich. Es bietet einen Überblick darüber, welche Systeme eingesetzt werden und folglich abgesichert werden sollten. Außerdem kann es auch für die Informationssicherheit Prozesse vereinfachen, wenn eine gewisse Integration zwischen dem Inventar und der Dokumentation im Rahmen eines Information Security Management System (ISMS) besteht.

Werden in ein Inventar auch Attribute hinsichtlich der Informationssicherheit übernommen, wie z. B. die Zugehörigkeit zu einem Schutzobjekt, kann das Inventar auch für die Erstellung und Pflege einer Strukturanalyse gemäß BSI-Standard 200-2 genutzt werden. Ebenso kann der Verweis in einem Inventareintrag auf das entsprechende Schutzobjekt im ISMS auch bei Audits hilfreich sein. So können Informationen schnell gefunden werden. Auch bei der Behandlung von Sicherheitsvorfällen ist eine schnelle Übersicht über alle erforderlichen Informationen wichtig.

Wenn die Erstellung und Pflege eines Inventars gut in die vorhandenen Prozesse eingebunden ist (Datenpflege schon in der Planungsphase, regelmäßige Aktualisierung, Aktualisierung bei

Neuanschaffung und Aussonderung etc.) kann das Inventar mit wenig Aufwand aktuell gehalten werden und bringt einen Mehrwert für viele Prozesse.

INF.13.M9 Regelung des Einsatzes von Computer-Aided Facility Management (S)

Computer-Aided Facility Management (CAFM) unterstützt das Facility Management durch geeignete Software. Mittels dieser Software können dem Facility Manager, aber auch externen Dienstleistern wichtige Informationen bezüglich ihrer Arbeitsbereiche und Aufgaben übersichtlich zugänglich gemacht werden. So können bei erfolgreichem Einsatz Arbeitsprozesse erleichtert, effizienter und kostensparender werden.

Wenn CAFM eingeführt wird, sollte dies bedarfsorientiert und zukunftsfähig erfolgen. Es sollte schon vor dem Einsatz geprüft werden, welche Aufgaben das CAFM übernehmen bzw. unterstützen soll und welche Konsequenzen dies hat (z. B. Zugriffe, Rollen, Berechtigungen, Daten). Dazu sollte unter anderem in einem Konzept festgehalten werden,

- wer das System nutzt, insbesondere ob hier Externe eingebunden werden,
- in welcher Art und Weise das System genutzt wird,
- wie oft es zu Veränderungen in den Nutzergruppen kommt,
- ob (webbasierte) Kundenportale benötigt werden und wie diese abgesichert sind,
- über welche Schnittstellen die Nutzer angebunden sind,
- welche Nutzer schon bei der Implementierung eingebunden werden sollten und
- welche Prozessschnittstellen oder Prozessbrüche es gibt.

Grundsätzlich lebt ein solches System von kontinuierlichen Anpassungen. Solche Änderungen müssen auch im Konzept nachgepflegt werden.

Nicht vergessen werden sollte auch immer eine entsprechende Schulung der Nutzerkreise, sodass auch hier eine abgestimmte und einheitliche Nutzung ermöglicht wird und der geplante Mehrwert tatsächlich möglich ist.

Da CAFM zur Verwaltung sicherheitsrelevanter Informationen und gegebenenfalls sogar zur Steuerung von Prozessen in Bezug zur Informationssicherheit verwendet wird, ist eine entsprechende Absicherung der CAFM-Systeme wichtig. Dies gilt insbesondere dann, wenn die CAFM-Systeme nicht nur der eigenen Institution, sondern auch externen Dienstleistern zur Verfügung stehen sollen. Um hier eine reibungslose und sichere Kommunikation zu ermöglichen, müssen Schnittstellen abgestimmt und definiert werden. Insbesondere solche Schnittstellen, die den Datentransfer ermöglichen, sind häufig Ziel von Angriffen und somit besonders zu schützen.

INF.13.M10 Regelung des Einsatzes von Building Information Modeling (S)

Building Information Modeling (BIM) ist eine Planungsmethode im Bauwesen, die auf einem objektorientierten 3D-Modell beruht. Diese Objekte bilden eine Informationsdatenbank zum gesamten Bauwerk und ermöglichen so die Abbildung des gesamten Lebenszyklus. BIM unterstützt somit auch die Planung von Prozessen und Verfahren und ermöglicht es, Risiken sowohl im Bau als auch im Betrieb frühzeitig zu erkennen und zu minimieren und die Wertschöpfungskette zu erhöhen.

Um tatsächlich von diesem Mehrwert profitieren zu können, ist es zunächst wichtig, dass alle Daten in BIM eingepflegt und aktuell gehalten werden. Sollten verschiedene Gewerke nicht in dem BIM-Modell integriert sein, ist die Aussagekraft der Methode deutlich reduziert. Eine Ausnahme bilden hier die Gewerke der Sicherheitsbranche. Daten zur Einbruchmeldetechnik, Brandmeldeanlage etc. sollten in der Projektorganisation (z. B. durch Teilprojekte) voneinander getrennt werden und nur für berechtigte Personen einsehbar sein.

Dementsprechend sollte es ein Rollen- und Berechtigungskonzept geben, das definiert, welche Rollen für BIM benötigt werden und welche Berechtigungen diesen Rollen zugewiesen werden. Dieses Rollen- und Berechtigungskonzept sollte dokumentiert und aktuell gehalten werden.

Wesentlich ist hier, dass BIM von der Planung bis zum Betrieb eines Gebäudes eingesetzt wird. Der Zugriff kann meist von verschiedenen Standorten aus gewährt werden, sodass Architekten, Ingenieure und alle weiteren involvierten Partner während der Planung und Ausführung sowie Betreiber- und Nachfrageorganisationen während der Betriebsphase auf die Informationen zugreifen können. BIM beinhaltet also sehr heterogene Daten und heterogene Nutzergruppen, die auf diese Daten zugreifen. Dadurch ist das Rollen- und Berechtigungskonzept für BIM wie auch für das TGM allgemein (siehe INF.13.M14 *Berücksichtigung spezieller Rollen und Berechtigungen im TGM*) etwas komplizierter als in der reinen IT.

Auch wenn der Zugang zu den BIM-Daten über Rollen und Berechtigungen geregelt wird, sollten sämtliche Daten verschlüsselt übertragen und gespeichert werden. So wird einem Angreifer der Zugriff auf BIM-Daten erschwert. Zusätzlich muss der Baustein CON.2 *Datenschutz* beachtet werden.

Wird eine Cloud-basierte BIM-Lösung genutzt, sollte auch hier sichergestellt werden, dass Daten gesichert und verschlüsselt übertragen und gespeichert werden. Hierzu muss der Baustein OPS.2.2 *Cloud-Nutzung* beachtet werden.

Basiert die BIM-Lösung auf Web-Anwendungen, muss der Baustein APP.3.1 *Webanwendungen* berücksichtigt werden.

Wichtig ist allgemein, dass der Umfang der eingesetzten BIM-Funktionen für jedes Projekt in einem BIM-Projektabwicklungsplan (auch BIM-Abwicklungsplan oder BIM-Ablaufplan, engl. BIM Execution Plan) konkret abgestimmt werden muss und dieser auch die Zusammenarbeit aller Beteiligten regelt. In einem BIM-Ablaufplan sollten mindestens folgende Punkte definiert sein.

- BIM-Ziele und Mehrwert
- BIM-Anwendungen
- BIM-Verantwortlichkeiten und Kontakte
- BIM-Zusammenarbeitsstrategie
- BIM-Qualitätsmanagement
- technische Vereinbarungen (Software, Formate)
- Vereinbarungen zu Austausch und Prozessen
- BIM-Leistungen

Damit die abgestimmten Abläufe eingehalten werden und eine phasenübergreifende Kommunikation stattfinden kann, wird in jedem BIM-Projekt ein BIM-Manager festgelegt. Der BIM-Manager, meist extern, leitet übergreifend den Bau schon ab der frühesten Planungsphase. Da dieser mit Abschluss der Bauphase meist aus dem Projekt ausscheidet, sollte für die Betriebsphase des TGM ein neuer (interner) BIM-Manager festgelegt werden.

Die Daten des BIM dienen oft auch als Datenquelle für die Gebäudedokumentation bzw. für ein CAFM-System (siehe INF.13.M9 *Regelung des Einsatzes von Computer-Aided Facility Management*).

INF.13.M11 Angemessene Härtung von Systemen im TGM (S)

Generell sollten für die Absicherung der TGM-Systeme sowie der TGA, die durch das TGM verwaltet wird, auch die entsprechenden SYS- bzw. IND-Bausteine berücksichtigt werden.

Für eine angemessene Härtung sollte je Systemtyp eine Checkliste mit den durchzuführenden Schritten zusammengestellt und abgearbeitet werden. Mindestens sollte diese Checkliste die folgenden Punkte berücksichtigen:

- Umsetzung der Herstellervorgaben zur Härtung

- Keine Speicherung von Passwörtern im Klartext
- Konfigurierbare Passwortkomplexität, sodass eigene Regelungen gemäß des Bausteins 4 *Identitäts- und Berechtigungsmanagement* festgelegt werden können (z. B. Minimallänge, beinhaltete Zeichen und Ziffern, keine Wiederverwendung)
- Deaktivierung von ungenutzten Diensten, Protokollen und Schnittstellen
- Keine Nutzung von unzureichend sicheren Protokollen (z. B. Telnet, TFTP, interne Web-Anwendungen via HTTP) Nutzung nur in abgesicherten Netzsegmenten; Deaktivierung der unzureichend sicheren Protokolle, wenn möglich
- Deaktivierung von Webservern oder Zugängen über Command Line Interface (CLI) mit unsicheren Protokollen; kann auf solche Webserver oder Zugänge über CLI nicht verzichtet werden, sollten sie zumindest angemessen abgesichert werden.
- Änderung von Default-Nutzern und Passwörtern

INF.13.M12 Sichere Konfiguration der TGM-Systeme (S)

Eine sichere Konfiguration der TGM-Systeme ist sehr wichtig, da insbesondere durch die Vielfalt der Systeme und Komponenten im TGM ein hohes Risiko für unentdeckte Angriffsmöglichkeiten besteht. Werden die Systeme von Anfang an sicher konfiguriert, kann das Risiko verringert werden.

Ein Test einer solchen Konfiguration kann bei einem Neubau vor der Inbetriebnahme, bei einem schon bestehenden Gebäude in einer Testumgebung stattfinden (siehe INF.13.M25 *Aufbau einer Testumgebung für das TGM*). Wird eine Konfiguration als sicher und vor allem auch sinnvoll angesehen, kann diese entsprechend automatisiert verteilt werden. Eine falsche Konfiguration kann insbesondere im TGM Sachschäden mit sich ziehen (z. B.: Auslösung von Sprinklersystemen zum falschen Zeitpunkt).

Insbesondere in Gebäuden, die mit Sensorik und intelligenten Systemen ausgestattet sind, fallen enorm viele Datenpakete an, die verarbeitet werden müssen. Um eine Überlastung von TGM-Systemen zu vermeiden, kann es sinnvoll sein, die erhobenen Daten schon so früh wie möglich zu aggregieren. Oftmals ist dies bereits schon durch eine passende Konfiguration des Elementes möglich. Beispielsweise können Daten jede Minute oder Stunde versendet werden, anstatt jede Millisekunde. Hochgerechnet auf die Vielzahl der durch das TGM zu überwachenden Systeme macht eine solche Anpassung der Konfigurationen einen großen Unterschied in der Datenlast.

Ist eine passende Konfiguration festgelegt, sollte diese unbedingt auch gespeichert werden, um in einem Notfall (z. B.: Ausfall der Systeme) schnell wiederhergestellt werden zu können. Der Speicherort dieser Konfigurationen sollte wenn möglich zentral und vom System abgekoppelt sein, damit dieser von einem eventuellen Ausfall oder Angriff nicht betroffen ist. Sollte eine Konfiguration nicht ohne weiteres gespeichert werden können, sollte sie entsprechend dokumentiert werden, um mit Hilfe der Dokumentation eine schnelle manuelle Wiederherstellung zu ermöglichen. Hier muss insbesondere beachtet werden, dass jede Änderung der Konfiguration nachgehalten wird. Um eine fehlerhafte Dokumentation zu vermeiden, sollte die Dokumentation regelmäßig auf Übereinstimmung mit der aktuellen Konfiguration geprüft werden. Wenn Abweichungen gefunden werden und die aktuelle Konfiguration sich als korrekt erweist, muss die Dokumentation umgehend entsprechend angepasst werden.

Allerdings sollte nicht nur die Dokumentation geprüft werden, sondern auch die Konfiguration selbst. Es kann durch Updates oder Patches vorkommen, dass Konfigurationen angepasst werden. Dies sollte zwar im Zuge des Tests vor einem solchen Change geprüft werden, allerdings ist auch hier ein regelmäßiger Test sinnvoll.

Manche Systeme erlauben es, eine zentrale Konfiguration zu erstellen, die dann systemweit automatisiert auf die kompatiblen Elemente verteilt werden. Somit ist es nicht mehr notwendig, jedes Element einzeln zu konfigurieren, sondern eine zentrale Verwaltung wird ermöglicht. Auch in diesem Fall sollten die Konfiguration und ihre sachgemäße Verteilung regelmäßig geprüft werden.

Außerdem ist es wichtig, dass jede Konfigurationsänderung allen Beteiligten an Serviceprozessen (Entstörung, Rufbereitschaft, Wartung etc.) bekannt ist, damit diese z. B. im Störungsfall aktuelle Kenntnisse haben und diese in die Fehlersuche einbeziehen können. Insbesondere die Änderung von Zugangsmechanismen oder Passwörtern muss allen Beteiligten mitgeteilt werden, damit ein Zugang jeder Zeit möglich ist.

INF.13.M13 Sichere Anbindung von eingeschränkt vertrauenswürdigen Systemen im TGM (S)

Im TGM kann es vorkommen, dass eingeschränkt vertrauenswürdige Systeme genutzt werden müssen. Dies kann beispielsweise der PC eines Wartungstechnikers sein oder auch ein älteres Bestandssystem, das als eingeschränkt vertrauenswürdig einstuft wird, da der Hersteller keine Patches mehr zur Verfügung stellt.

Zunächst ist es notwendig das System selbst oder die damit verbundenen Geräte soweit wie möglich zu härten. Dazu sollten Einstellungen geprüft werden und nicht benötigte Funktionen, wenn möglich deaktiviert werden.

Zudem ist es sinnvoll, eingeschränkt vertrauenswürdige Systeme in eigene Netzwerksegmente einzubinden und somit über eine Firewall die Kommunikationsmöglichkeiten einzuschränken. So können beispielsweise nur explizit erwünschte und als sicher eingestufte IP-Adressen und Ports zugelassen werden.

Dennoch sollte die Anbindung von eingeschränkt vertrauenswürdigen Systemen soweit möglich reduziert werden. Es kann vorkommen, dass alte Bestandssysteme in neue Netze eingebunden werden müssen. Bei Neuanschaffungen muss allerdings darauf geachtet werden, dass diese vertrauenswürdig und sicher einbindbar sind.

INF.13.M14 Berücksichtigung spezieller Rollen und Berechtigungen im TGM (S)

Durch die Gemengelage im TGM gibt es hier meist mehr Beteiligte als in der sonstigen IT. Daher sollten auch im Rollen- und Berechtigungskonzept hinsichtlich des TGM alle Beteiligten berücksichtigt werden. Hier sollten nicht nur die Ausführenden des TGM (Betreiberorganisation TGM) bedacht werden, sondern gegebenenfalls auch Nachfrageorganisationen und weitere Betreiberoganisationen der TGA-Systeme. Diese benötigen gegebenenfalls zumindest lesenden Zugriff auf Informationen.

Im TGM sollten daher entsprechende Rollen und damit verbundene Berechtigungen berücksichtigt werden. Das erhöht die Sicherheit im TGM und schützt unter anderem vor ungewollten Änderungen bei unqualifiziertem Zugriff auf die Systeme.

Üblicherweise werden mindestens die folgenden drei Stufen unterschieden:

- Lesender Zugriff
- Zugriff mit Änderungs-Berechtigung
- Voller Zugriff samt möglicher Neuanlage oder Löschberechtigung

Die dritte Stufe wendet sich meist ausschließlich an besonders qualifizierte Personen, Administratoren oder ähnliche Personenkreise, um Fehlbedienungen oder Fehlkonfigurationen zu vermeiden bzw. zu reduzieren.

Neben den oben vorgeschlagenen Abstufungen sind natürlich weitaus breiter aufgestellte Einstufungen möglich, je nach Anwendungsfall. Eine neue Rolle sollte immer dann eingeführt werden, wenn mehrere Benutzer die gleichen Berechtigungen bekommen sollen. Im Idealfall wird einer Rolle dabei genau das Minimum der benötigten Berechtigungen erteilt.

Benutzer können einer oder sogar mehreren Rollen zugeteilt werden. Diese Zuteilung kann laufend angepasst werden.

Die Zuordnung von Benutzer zu Rolle und Berechtigung erfolgt mittels einer Anmeldung an bzw. eines Logins in das jeweilige TGM-System. So können die Daten entsprechend abgeglichen werden und die Berechtigungen zugewiesen werden. Insbesondere für die Nutzer mit einer hohen Berechtigungsstufe ist es dementsprechend umso wichtiger, eine angemessene Authentisierung und Passwortkomplexität einzuhalten, um unbefugte Zugriffe zu vermeiden. Eine Sperrung des Accounts bei einer vordefinierten Anzahl erfolgloser Login-Versuche ist ebenfalls sinnvoll.

Oftmals greifen Änderungen in den Berechtigungen erst, wenn Nutzer ausgeloggt sind. Daher wird ein Auto-Log-out bei Nichtbenutzung sehr empfohlen.

Auch für technische Benutzer im TGM, d. h. für die Maschine-Maschine-Kommunikation, sollten in ähnlicher Weise Rollen und Berechtigungen festgelegt werden.

Allgemein sollte für Rollen und Berechtigungen der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* berücksichtigt werden.

INF.13.M15 Schutz vor Schadsoftware im TGM (S)

Auf manchen Systemen, die durch das TGM verwaltet werden, ist es nicht möglich, fremde Software und somit Virenschutzprogramme oder Ähnliches zu installieren. Daher sollten dann alternative Schutzverfahren eingesetzt werden.

Beispielsweise sollte ein Zugriff auf diese Systeme aus nicht vertrauenswürdigen Netzen, wenn möglich, unterbunden werden. Außerdem sollten solche Systeme als eingeschränkt vertrauenswürdige Systeme gemäß INF.13.M13 *Sichere Anbindung von eingeschränkt vertrauenswürdigen Systemen im TGM* separiert werden. Dann können die Kommunikationsmöglichkeiten über Firewall eingeschränkt werden und Schadsoftware kann sich zumindest nur in dem entsprechenden Netzsegment ausbreiten.

Auch eine generelle Absicherung des Netzes gegen den Anschluss fremder Geräte, z. B. in Form einer Netzzugangskontrolle, kann den Schutz vor Schadsoftware erhöhen. Genauso sollte auch jeder externe Datenträger auf Schadsoftware geprüft werden, bevor er in ein System eingesteckt wird und Daten übertragen werden.

Zudem sorgen regelmäßige Updates der betroffenen Systeme auch für eine gewisse Absicherung, indem Sicherheitslücken geschlossen werden und somit Schadsoftware daran gehindert wird, in die Systeme einzudringen. Regelmäßige Updates sollten zudem vor dem Ausrollen entsprechend getestet werden, um einen reibungslosen Ablauf und eine Fehlerfreiheit nach dem Update sicherzustellen. Weiterhin sollten Updates nur von zuverlässigen Quellen heruntergeladen und akzeptiert werden. So ist auch hier die Gefahr reduziert, dass durch ein beeinträchtigtes Update Schadsoftware in das System gelangt.

Regelmäßige Backups helfen zudem dabei, ein System im Falle eines Angriffs durch Schadsoftware wieder in den ursprünglichen Zustand zurück zu versetzen. Die Häufigkeit dieser Backups sollte je nach Schutzbedarf der Umgebung entsprechend angepasst werden. Ein sicherer Aufbewahrungsort von Backups ist ebenso wichtig wie regelmäßige Tests, ob Backups auch problemlos wieder eingespielt werden können.

Außerdem trägt ein abgestimmtes Rollen und Berechtigungskonzept dazu bei, unbefugte Zugriffe und somit das Risiko von bewusst oder unbewusst eingebrachter Schadsoftware zu reduzieren.

INF.13.M16 Prozess für Änderungen im TGM (S)

Es ist wichtig, Änderungen an TGA-Systemen immer anzukündigen und mit allen beteiligten Gewerken, Betreiber- und Nachfrageorganisationen abzustimmen, die von den Änderungen betroffen sein könnten. In einem Gebäude gilt dies als besondere Herausforderung, da hier besonders viele Gewerke voneinander abhängig sind. Um hier problematische Wechselwirkungen zu vermeiden, bietet es sich an, eine entsprechende Testumgebung aufzubauen, um Änderungen vor ihrem Inkrafttreten zu testen (siehe dazu INF.13.M25 *Aufbau einer Testumgebung für das TGM*).

Auch die Möglichkeit für einen Rückbau der Änderungen sollte im Vorfeld getestet werden, da es in der TGA Systeme gibt, die nicht auf eine vorherige Version zurückgesetzt werden können (z. B. gewisse

Direct Digital Controller, DDCs). Änderungen an solchen Systemen sind besonders kritisch und sollten angemessen getestet werden, damit keine Probleme auftreten. Die Testtiefe ist abhängig von der Art der Änderung und sollte für verschiedene typische Änderungen festgelegt werden. Außerdem sollte insbesondere bei Systemen, für die kein Rückbau möglich ist, ein Vorgehen geplant werden für den Fall, dass trotz durchgeführter Tests Probleme auftreten.

Eine weitere Herausforderung ist der Zeitpunkt einer Änderung. Üblicherweise gibt es Wartungsfenster, die eingehalten werden müssen. In Gebäuden gibt es kaum ungenutzte Zeiträume, in denen problemlos Änderungen durchgeführt werden können. Daher müssen die Änderungen meist parallel zur produktiven Nutzung durchgeführt werden. Auch hier sind Tests der Änderungen in einer Testumgebung sinnvoll. Ist dies nicht möglich, sollte zumindest ein Vorgehen zur Behebung möglicher Probleme geplant werden.

Generell sollten mindestens nach Abschluss einer Änderung alle betroffenen Funktionen getestet werden. Der Umfang dieser Tests und die Testtiefe variieren je nach Größe, Art und Dringlichkeit der Änderung (siehe INF.13.M22 *Durchführung von Systemtests im TGM*).

INF.13.M17 Regelung von Wartungs- und Reparaturarbeiten im TGM (S)

Da die Gebäudeeinrichtungen die technische Funktion und Verfügbarkeit eines Gebäudes bedingen, ist ihre regelmäßige Wartung besonders wichtig. Meist ist die Wartung auch Bestandteil von Vorschriften oder Bedingung für entsprechenden Versicherungsschutz.

Ein Wartungsplan ist wesentlich, um passende Wartungsfenster zu finden und mit den beteiligten Personen abzustimmen, vorgeschriebene Fristen nicht zu vergessen und die anstehenden Arbeiten zu koordinieren. Nicht nur das meist externe Wartungspersonal muss verfügbar sein, sondern auch interne Mitarbeiter zur Autorisierung, Beobachtung, gegebenenfalls Unterstützung und Abnahme der Arbeiten. Eventuell ist auch eine externe Abnahme, z. B. TÜV erforderlich, um die gesetzlichen Bestimmungen zu erfüllen, oder die Arbeiten dürfen nur von nachweislich qualifizierten Firmen durchgeführt werden. Dies gilt auch für Reparaturarbeiten. Die entsprechenden Zuständigkeiten und Bedingungen sowie Ansprechpartner sollten aktuell und verfügbar mit entsprechenden Zugriffsregelungen dokumentiert sein, ebenso die durchgeführten Wartungs- oder Reparaturarbeiten.

Sowohl bei Wartungsarbeiten als auch bei Reparaturarbeiten müssen Abhängigkeiten berücksichtigt werden und alle betroffenen Bereiche informiert werden. Wird z. B. die Klimatisierungsanlage gewartet, sollten die Zuständigen für ein RZ oder IT-Verteilerräume im Gebäude informiert sein, um die Temperaturen überwachen und gegebenenfalls Gegenmaßnahmen ergreifen zu können.

Ebenso wichtig ist es, sinnvolle oder insbesondere vorgeschriebene Sicherheitsmaßnahmen sowohl für das Wartungspersonal als auch für Unbeteiligte einzuhalten. Eventuell sind Bereiche abzusperren oder Informationsschilder aufzustellen.

Gerade bei einer 24x7-Verfügbarkeit sollten einfache Wartungs- und Reparaturarbeiten, wie z. B. der Austausch eines Rauchmelders oder der Neustart eines Systems, sofort durch das gerade anwesende Personal, eventuell mit telefonischer Unterstützung, erledigt werden können. Hierfür ist es wichtig, die entsprechenden Prozesse und Mechanismen für diese einfachen Wartungs- und Reparaturarbeiten an die Qualifizierung der entsprechenden Mitarbeiter vor Ort anzupassen bzw. im Umkehrschluss die entsprechenden Mitarbeiter dahingehend zu schulen, dass sie diese anfallenden Arbeiten erledigen können.

INF.13.M18 Proaktive Instandhaltung im TGM (S)

Eine proaktive Instandhaltung soll Ausfälle von Systemen vermeiden, indem diese Systeme oder Teile von ihnen bei regelmäßigen Wartungen vorsorglich zeitabhängig ausgetauscht werden, bevor sie ausfallen. Abhängig von der Lebensdauer von Systemen oder deren Komponenten und vom Schutzbedarf der Systeme sollten individuelle Wartungsintervalle festgelegt werden. Bei einer solchen Wartung im Rahmen der proaktiven Instandhaltung sollte mindestens Folgendes geprüft werden und gegebenenfalls ein vorsorglicher Austausch vorgenommen werden:

- Vorhandensein von End-of-Life- oder End-of-Service-Meldungen (EoL- oder EoS-Meldungen) für das System oder eine seiner Komponenten
- Über- bzw. Unterschreiten von Parametern eines Systems oder einer seiner Komponenten, z. B. bei der Laufzeit eines Lüfters

Weiterhin sollten

- die Laufzeit von Zertifikaten und gegebenenfalls bestehenden zeitlich begrenzten Nutzerzugängen sowie
- die Nutzung mittlerweile aus Sicherheitsgründen nicht mehr erlaubter Nutzerzugänge

überprüft werden.

Fehlende Sicherheitsupdates sollten nachinstalliert werden. Ist dies nicht möglich, sollte eine Strategie für den Umgang mit den entsprechenden Systemen entwickelt werden. Im Rahmen dieser Strategie sollte auch in Betracht gezogen werden, solche Systeme gegen neue Systeme zu ersetzen.

Eine solche Überprüfung bietet auch eine gute Gelegenheit für einen Soll-Ist-Vergleich zwischen Vorgaben von Konzepten und aktuellem Zustand.

Gerade in kleineren Außenstellen ist es wichtig, die Prozesse und Austauschmechanismen für die proaktive Instandhaltung an die Qualifizierung der Mitarbeiter vor Ort anzupassen bzw. im Umkehrschluss die entsprechenden Mitarbeiter dahingehend zu schulen, dass sie die anfallenden Arbeiten erledigen können.

Bei der vorausschauenden Instandhaltung (Predictive Maintenance) wird der Zustand von in Betrieb befindlichen Systemen analysiert, um vorherzusagen, wann eine Instandhaltungsmaßnahme durchgeführt werden sollte. Dabei ist ein Parameter die Schätzung der Wahrscheinlichkeit einer Störung in einem gewissen Zeitraum, die den Austausch einer Komponente bedingen würde. Übersteigt diese Schätzung einen gewissen Schwellwert, wird die Komponente bei einem Wartungsfenster ausgetauscht, auch wenn sie augenscheinlich noch funktioniert. Auf diese Weise sollen einerseits Störungen proaktiv vermieden werden und andererseits sollen unnötige häufige Wartungen reduziert werden, was durchaus zu Kosteneinsparungen bei gleichzeitiger Qualitätsverbesserung führen kann.

Standardmäßig wird bei einem solchen Vorgehen nach von der Norm abweichendem Verhalten von Systemen gesucht. Dieses kann dann vom Menschen oder maschinell ausgewertet werden. Besonders interessant ist diese Vorgehensweise durch den Einsatz von Künstlicher Intelligenz (KI) geworden, da hier komplexere Szenarien betrachtet werden können und weitergehende Korrelationen feststellbar sind. Daher wird abhängig von der Komplexität des Systems für eine solche Vorhersage des Systemzustands vielfach eine dem Einsatzzweck angemessene KI eingesetzt, die mit KI-Methoden die Prüfung und Auswertung vornimmt. Diese KI-Methoden sind oft cloudbasiert und in der Regel herstellergebunden. Die Daten des zu prüfenden Systems werden erfasst, digitalisiert, an die KI übermittelt und bei einer selbstlernenden KI letztendlich auch quasi gespeichert. Die KI analysiert und bewertet die erhobenen Daten und errechnet Eintrittswahrscheinlichkeiten für bestimmte Ereignisse. Hier sollte eine qualitativ hochwertige und dem Schutzbedarf entsprechend sichere KI eingesetzt werden (siehe INF.13.M28 *Sichere Nutzung von Künstlicher Intelligenz im TGM*).

INF.13.M19 Konzeptionierung und Durchführung des Monitorings im TGM (S)

Die Konzeptionierung des Monitorings im TGM beginnt schon bei der Anforderungsanalyse. Hier sollte sichergestellt werden, dass anzuschaffende Systeme in die vorgesehene Monitoring-Lösung eingebunden werden können und dass sich die gewünschten Werte und Schnittstellen wie geplant überwachen lassen.

Oftmals können nicht alle Systeme in ein Monitoring eingebunden werden, z. B. aufgrund mangelnder Protokoll-Unterstützung. Das ist insbesondere im Bereich des Internet of Things (IoT) manchmal der Fall. Hier sind die verwendeten Geräte oft zu beschränkt und minimal aufgebaut, um weitere

zusätzliche Monitoring-Protokolle unterstützen zu können. Dennoch sollte versucht werden, zumindest die Verfügbarkeit dieser Systeme überwachen zu können.

Für das Monitoring sollte insbesondere die Produktvielfalt beachtet werden, die es typischerweise in der TGA gibt. Es sollten so viele Systeme wie möglich in eine einheitliche Monitoring-Lösung eingebunden werden. Einen Überblick über alle Systeme bietet das Inventar (siehe INF.13.M8 *Erstellung und Pflege eines Inventars für das TGM*). Möglicherweise ist es aber auch notwendig, verschiedene Monitoring-Lösungen zu verbinden, um das Spektrum der eingesetzten Systeme und Produkte abdecken zu können. In diesem Fall ist es umso wichtiger, ein abgestimmtes Konzept vorweisen zu können, in dem auch die Zusammenarbeit der Monitoring-Lösungen spezifiziert wird.

Die organisatorische Hoheit über das Monitoring hängt von der Organisationsstruktur innerhalb des Gebäudes ab und ist aufgrund der Gemengelage individuell sehr unterschiedlich. Gegebenenfalls sollten Vereinbarungen darüber getroffen werden, inwieweit Mitspracherechte bestehen, eine Einsichtnahme in Monitoringdaten erfolgen soll oder Alarme in andere Bereiche weitergeleitet werden sollen.

Nicht zuletzt sollte in Betracht gezogen werden, auch die eingesetzte Monitoring-Lösung selbst von einem weiteren System zu überwachen, um sicherzustellen, dass sie selbst erreichbar ist und wie vorgesehen funktioniert.

Ist eine passende Monitoring-Lösung für die TGA aufgebaut und konzeptioniert, kann diese auch zur präventiven Instandhaltung der Systeme und Komponenten beitragen (Predictive Maintenance, siehe INF.13.M18 *Proaktive Instandhaltung im TGM*). Hier werden anhand von regelmäßigen Messungen entsprechende Baselines erstellt, sodass eine Abweichung vom Normalzustand schnell erkannt werden kann. So kann in vielen Fällen schon vor dem Defekt eines Gerätes auf den schlechter werdenden Zustand hingewiesen werden. Dementsprechend können Ersatzkomponenten, Personal etc. rechtzeitig beschafft werden, und einem Ausfall oder Defekt bzw. deren Auswirkungen wird vorgegriffen.

INF.13.M20 Regelung des Ereignismanagements im TGM (S)

Ein Ereignis ist eine Statusänderung, eine Alarmmeldung oder eine Benachrichtigung, die durch ein System gegebenenfalls zunächst nur lokal aufgezeichnet oder aber selbständig an ein Monitoring-System gesendet bzw. vom Monitoring-System selbst bei der Abfrage eines Systems generiert wird. Da gerade im TGM eine Vielzahl solcher Ereignisse von unterschiedlichsten Systemen generiert wird, ist ein zentrales systemübergreifendes Monitoring von besonderer Bedeutung, das unablässig diese Ereignismeldungen kategorisiert, filtert und priorisiert. Beispielsweise muss nicht auf jede Gradänderung der Raumtemperatur reagiert werden, wenn aber eine gewisse vorgegebene Temperatur, der Schwellwert, über- oder unterschritten wird, ist ein Eingreifen erforderlich. Beispiele für Ereignis-Kategorien sind:

- Information
- Warnung
- Fehler

Prinzipiell sollten für jeden Systemtyp den möglichen Ereignissen Kategorien zugeordnet werden, für die dann eine weitere Behandlung im Ereignismanagement spezifiziert werden kann. Häufig werden hierfür Schwellwerte oder ein Punktesystem festgelegt, bei deren Über- oder Unterschreitung die Kategorie z. B. von Information zu Warnung wechselt. Dies kann auch automatisiert erfolgen und dabei für die Weiterbehandlung unwichtige Ereignisse herausfiltern.

Gegebenenfalls ist aufgrund der Gemengelage im Gebäude eine Absprache bezüglich der Kategorisierung der Ereignisse mit allen Beteiligten erforderlich.

Tritt eine Warnung bzw. ein Fehler auf, sollte eine geregelte Übergabe an das Incident-Management erfolgen. Solche Schnittstellen sollten im Vorfeld genau spezifiziert werden, um die Incident-Behandlung möglichst effektiv beginnen zu können. Beispielsweise könnte im Vorfeld schon festgelegt werden, welche Daten übergeben werden müssen, sollte es sich um einen Fehler handeln. Hier ist es natürlich von Vorteil, wenn sämtliche Systeme wie in INF.13.M8 *Erstellung und Pflege eines Inventars*

für das TGM beschrieben, bereits inventarisiert und somit viele Daten bereits verfügbar sind und nicht erst bei der Incident-Behandlung manuell recherchiert werden müssen.

INF.13.M21 Protokollierung im TGM (S)

Im TGM werden auf den einzelnen Systemen oft große Mengen von Ereignissen generiert und entsprechende Daten protokolliert. Diese sollten durch das Ereignismanagement (siehe auch INF.13.M20 *Regelung des Ereignismanagements im TGM*) auf wesentliche Daten eingeschränkt und insbesondere diese Ereignisse sollten dann an eine zentrale Protokollierungsinstanz weitergeleitet werden. Ansonsten entstehen potentiell auf der einen Seite eine nicht zu unterschätzende Netzlast und auf der anderen Seite eine sehr große und unübersichtliche Menge an Protokollierungsdaten, die größtenteils für eine Weiterbearbeitung uninteressant sind.

Allerdings sollten sicherheitsrelevante Ereignisse auf jeden Fall an eine zentrale Protokollierungsinstanz weitergeleitet werden. Außerdem sollten bei sicherheitskritischen Ereignissen auch automatisiert die zuständigen Administratoren alarmiert werden, z. B. per E-Mail, SMS oder über Pager, damit sofort geeignete Maßnahmen ergriffen werden können. Auch ein Alarm an eine übergeordnete Managementstation, zu übergreifenden Werkzeugen im IT-Betrieb oder an einen Leitstand oder Helpdesk ist möglich.

Die Protokollierung von Anmeldungen mit privilegierten Konten und entsprechender Zugriffe inklusive Konfigurationsänderungen sowie von manuellen und automatisierten Steuerungszugriffen ist für verschiedene Ziele wichtig und sollte daher stets erfolgen. Zum einen können auf diese Weise Konfigurations- und Steuerungsänderungen im Nachhinein mit auftretenden Fehlern korreliert werden um gegebenenfalls Zusammenhänge aufzudecken. Zum anderen können so auch unautorisierte Zugriffe erkannt werden.

Grundsätzlich sollte die Protokollierung im TGM gemäß Baustein OPS.1.1.5 *Protokollierung* erfolgen.

INF.13.M22 Durchführung von Systemtests im TGM (S)

Bei jedem Test ist es wichtig, dass berücksichtigt wird, ob auch notwendige Sicherheitsaspekte in den Testfällen systematisch überprüft werden, die insbesondere allgemein in Sicherheitsrichtlinien oder detaillierter in Sicherheitskonzepten oder Anforderungskatalogen einer Ausschreibung gefordert werden. Diese Dokumente beschreiben, was in einem System als sicher oder als unsicher gilt und was mit verschiedenen Tests daher belegt oder widerlegt werden kann. Dies gilt bei Tests von einzelnen kleineren Softwarekomponenten (ggf. sogar auf Quelltextniveau), aber insbesondere bei Tests des gesamten Systems, sogenannten Systemtests.

Je nach Hintergrund sind bei einem Systemtest verschiedene Testtiefen sinnvoll. Es muss bei jedem Systemtest festgelegt werden, in welcher Testtiefe und Testbreite dieser erfolgen soll. Beispielsweise reicht bei einem kleinen Change ein weniger umfangreicher Test wie ein sogenannter Smoke Test aus, der im Sinne eines grundlegenden Probelaufs lediglich die elementare Funktionsfähigkeit prüft. Sollte allerdings ein komplettes System neu in Betrieb genommen werden, ist im Rahmen eines Abnahmetests eine sehr viel höhere Testtiefe notwendig. Hier sollten auch Details und Schnittstellen geprüft und gegebenenfalls Negativ-Tests (wie verhält sich das System unter ungewöhnlichen Eingaben) durchgeführt werden, um die Sicherheit und Funktionsfähigkeit eines Systems festzustellen.

Bei Systemtests sollten bei einer größeren Testtiefe also nicht nur funktionale Aspekte berücksichtigt werden, sondern auch Aspekte der Dimensionierung und Sicherheitsaspekte wie Verfügbarkeit (beispielsweise mit Last- oder Stresstests) und zielgerichtete Tests, um Vertraulichkeit und Integrität zu prüfen. Je nach Testtiefe kann hier auch ein Schwachstellentest oder auch ein Penetrationstest sinnvoll sein. Dazu sollte INF.13.M23 *Integration des TGM in das Schwachstellenmanagement* bzw. INF.13.M30 *Durchführung von Penetrationstests im TGM* beachtet werden.

Auch Tests, die die Konfiguration von Parametern der Informationssicherheit betreffen, müssen berücksichtigt werden. Beispiele hierfür sind:

- Prüfung der Passwortkomplexität für Konten
- Prüfung, ob das Default-Passwort tatsächlich ersetzt wurde

- Prüfung, ob Verschlüsselungen aktiviert sind

Allgemein müssen sich Tests an den für TGM definierten Prozessen orientieren. Zum Beispiel können Produkte erst in die Prozesslandschaft eingebunden werden, wenn entsprechende Tests bestanden sind.

Für alle Tests, die durchgeführt oder geplant werden, muss es eine Testdokumentation geben. In dieser werden die geplanten Tests in einer Testspezifikation festgehalten, die Testumgebung beschrieben und insbesondere auch die Ergebnisse der Tests festgehalten und bewertet.

INF.13.M23 Integration des TGM in das Schwachstellenmanagement (S)

Schwachstellen, die Angriffe begünstigen und damit zu Fehlern, Störungen oder Ausfällen führen können, können im TGM durch die hohe Vernetzung weitreichende Folgen haben. Daher sollten die Systeme des TGM und die durch das TGM verwalteten Systeme fortlaufend hinsichtlich möglicher Schwachstellen überwacht werden. Dies kann auf verschiedene Weise geschehen.

Mindestens sollten regelmäßig Informationen über bekannt gewordene Schwachstellen eingeholt werden. Diese müssen dann auf Relevanz geprüft werden für die Systeme des TGM und für die Systeme, die durch das TGM verwaltet werden. Hierfür ist es hilfreich, wenn die für diese Prüfung benötigten Informationen über die eingesetzten Systeme, wie z. B. der Software-Stand, übersichtlich in einem Inventar (siehe INF.13.M8 *Erstellung und Pflege eines Inventars für das TGM*) gelistet sind und nicht erst mühsam herausgesucht werden müssen. Außerdem wird auf diese Weise auch kein System vergessen.

Weiterhin können unübliche Netzaktivitäten, also jegliche Abweichungen von der Norm, darauf hindeuten, dass gerade Schwachstellen ausgenutzt werden. Solche Abweichungen können beispielsweise über das Monitoring oder die Protokollierung erkannt werden.

Außerdem können Schwachstellen-Scans eingesetzt werden. Hier muss zwischen aktiven und passiven Scans unterschieden werden. Bei aktiven Scans wird aktiv über das Netz auf die getesteten Systeme zugegriffen, um Schwachstellen zu erkennen. Diese Zugriffe können die betroffenen Systeme aber auch beeinträchtigen, indem sie z. B. Kapazitäten binden, die dann nicht mehr für die eigentlichen Aufgaben der Systeme verfügbar sind. Auch der zusätzlich entstehende Netzverkehr kann ein Problem darstellen. Im schlimmsten Fall kann es zu System- oder Netzausfällen kommen. Passive Scans hingegen analysieren den Netzverkehr, indem der Netzverkehr der Systeme, die vom Scanner untersucht werden sollen z. B. über einen Mirror Port oder einen Tunnel zum Scanner gespiegelt wird. Sie beeinträchtigen die untersuchten Systeme nicht, erzeugen jedoch je nach eingesetzter Technik für die Anbindung der Switches an den Scanner gegebenenfalls erheblichen zusätzlichen Netzverkehr. Dies sollte möglichst bereits in der Planung des TGM berücksichtigt werden.

Daher sollten in Produktivumgebungen passive Schwachstellen-Scans bevorzugt werden. Aktive Schwachstellen-Scans sollten genau wie Penetrationstests (siehe auch INF.13.M30 *Durchführung von Penetrationstests im TGM*) möglichst in einer Testumgebung durchgeführt werden. Lässt sich ihr Einsatz in einer Produktivumgebung nicht vermeiden, sollten sie zumindest umfassend geplant und alle Betroffenen informiert werden.

Um den Aufwand dem Nutzen anzupassen, sollte im Vorfeld geprüft werden, welche Systeme besonders kritisch oder anfällig sind. Für diese sollten häufigere Scans vorgesehen werden, die meist auch entsprechend tiefer gehen sollten. Bei weniger anfälligen oder kritischen Systemen kann ein Scan bei Inbetriebnahme und großen Systemänderungen ausreichen. Gegebenenfalls können in diesem Fall auch weniger tiefgehende Scans gewählt werden. Entsprechende Entscheidungen sollten begründet dokumentiert, regelmäßig überprüft und gegebenenfalls angepasst werden.

Alle gefundenen Schwachstellen sollten in das Schwachstellenmanagement der Institution aufgenommen und bewertet werden. Wenn Schwachstellen behoben werden können, indem z. B. ein Patch eingespielt werden kann, sollte dies umgehend erfolgen und die betroffene Dokumentation entsprechend angepasst werden. Schwachstellen, die nicht schnell genug behoben werden können, sollten gemäß ihres Schweregrads in das Risikomanagement der Institution aufgenommen und dabei auch Maßnahmen erarbeitet und umgesetzt werden, die das Risiko reduzieren.

INF.13.M24 Sicherstellung der Kontrolle über die Prozesse bei Cloud-Nutzung für das TGM (S)

Um die Kontrolle über Prozesse bei der Cloud-Nutzung für das TGM sicherzustellen, sollten die Anforderungen gemäß aktuellem BSI Kriterienkatalog Cloud Computing (C5) [BSI C5] und die Anforderungen aus dem Baustein OPS.2.2 *Cloud-Nutzung* umgesetzt werden. Diese gelten sowohl wenn die IT der Institution als Cloud-Betreiber fungiert als auch für externe Cloud-Provider.

Wird ein externer Cloud-Provider genutzt, sollte sichergestellt werden, dass dieser den Sicherheitsanforderungen des TGM genügt. Dies kann z. B. bedeuten, dass die Speicherung der Daten ausschließlich in der Europäischen Union erfolgen darf. Generell gilt jedoch, dass Datensicherungs- und Wiederherstellungsprozesse vorhanden sein sollten. Darüber hinaus sollte abgewogen werden, ob und welche nachgelagerten Cloud-Dienste, z. B. zur Speicherung von großen Datenmengen, genutzt werden dürfen.

Ein weiterer Punkt, der abgestimmt und analysiert werden sollte, ist die Verwendung von sicheren Protokollen bei der Cloud-Nutzung. Hierzu sollte INF.13.M5 *Planung des TGM* beachtet werden. Ebenso müssen Anforderungen an die Verfügbarkeit abgestimmt werden.

Allgemein ist es nicht nur wichtig, die Kontrolle über die Prozesse dem Cloud-Provider gegenüber sicherzustellen, sondern ebenfalls gegenüber weiteren Instanzen im TGM, die beispielsweise in die Bereitstellung des Cloud-Zugangs involviert sind.

Grundsätzlich sollte eine umfassende Analyse der Abhängigkeiten von der Cloud-Anbindung durchgeführt werden und auf Basis dieser Analyse zwischen verschiedenen Cloud-Nutzungsformen entschieden werden. Beispielsweise kann das TGM eine eigene Cloud über eine dedizierte Internetanbindung oder über einen zentralen Internetzugang der Institution nutzen, oder aber eine zentrale Cloud-Anbindung der Institution.

INF.13.M25 Aufbau einer Testumgebung für das TGM (H)

Es gibt meist keine Zeiten, an denen ein Gebäude vollständig ungenutzt ist. Daher ist es schwer möglich, Wartungsfenster oder ähnliches zu definieren. Um die Produktivumgebung mit Tests nicht zu beeinträchtigen oder zu zerstören, sollte eine Testumgebung aufgebaut werden. Insbesondere Negativ-Tests, also Tests, in denen Systeme mit nicht konformen Daten, Einstellungen etc. auf ihre Stabilität und Sicherheit getestet werden, führen oftmals zu Abstürzen oder Defekten. Auch Last- und Stresstests können für enorme Beeinträchtigungen sorgen, wenn diese in der Produktivumgebung durchgeführt werden.

Im TGM gibt es die zusätzliche Herausforderung, dass eine Fehlfunktion der Systeme Gefahr für Leib und Leben bedeuten kann. Daher ist es notwendig, mit Testumgebungen zu arbeiten, auch wenn dies entsprechende Investitionen bedeutet. Im TGM kommt hinzu, dass es sich meist um heterogene Umgebungen handelt, die Systeme und Komponenten also sehr unterschiedlich sind. Daher werden meist umfangreichere Testumgebungen benötigt und die Kosten sind höher als in homogenen Umgebungen.

Sollte es nicht möglich sein, eine Testumgebung aufzubauen, ist eine gute Planung der Tests enorm wichtig. Bei Fehlfunktionen muss schnell eingegriffen werden können und im schlimmsten Fall muss das System schnell wiederhergestellt werden können. Das Risiko sollte dementsprechend minimiert werden. Aggressive Tests (wie die oben beschriebenen Negativ-Tests) sollten nur innerhalb einer Testumgebung ausgeführt werden.

Trotz aller Vorkehrungen kann die Testumgebung allerdings die realen Gegebenheiten nur bedingt abbilden. In Produktivumgebungen gibt es weitaus mehr Variablen, die auch nach gründlichen Tests in einer Testumgebung noch zu ungeplanten Auswirkungen führen können.

INF.13.M26 Absicherung von BIM (H)

Bei der Nutzung von BIM werden meist auch sicherheitskritische Daten gespeichert, wie zum Beispiel IP-Adressen, MAC-Adressen, Personenbezüge (Name, Telefonnummer für Zuständigkeit) oder auch

Daten zur Raumnutzung. Insbesondere in diesem Fall ist eine Absicherung der BIM-Systeme und BIM-Daten sehr wichtig, zum Beispiel mittels einer 2-Faktor-Authentisierung oder generell einer Verschlüsselung sowohl der Daten als auch der Transportwege.

Um Daten vor unbefugtem Zugriff zu schützen, ist ein dediziertes Netzsegment für BIM sinnvoll.

Auch eine Ereignisprotokollierung, die jegliche administrativen Zugriffe berücksichtigt, muss aktiviert und entsprechend eingestellt werden. Hierzu sollte insbesondere der Baustein OPS.1.1.5 *Protokollierung* beachtet werden. Diese Informationen sollten in eine zentrale Protokollierung eingebunden werden und somit auch in ein SIEM übertragen werden. Hierzu sollte insbesondere INF.13.M29 *Integration des TGM in ein SIEM* berücksichtigt werden.

INF.13.M27 Einrichtung einer Private Cloud für das TGM (H)

Im TGA-Umfeld werden häufig Cloud-Dienste für das Management der Systeme genutzt. Im schlimmsten Fall hat jedes TGA-System einen eigenen Cloud-Dienst. Dadurch entsteht schnell eine heterogene, unübersichtliche Cloud-Dienst-Landschaft, die einen erheblichen Abstimmungsaufwand erfordert und hohe Sicherheitsrisiken mit sich bringt. Daher sollten zumindest bei erhöhtem Schutzbedarf Cloud-Dienste zum TGM in einer Private Cloud On-Premises oder einer Private Cloud bei einem vertrauenswürdigen Cloud-Anbieter positioniert werden.

Für die Einrichtung und Nutzung der Private Cloud sollten die Anforderungen gemäß aktuellem BSI Kriterienkatalog Cloud Computing (C5) [BSI C5] und die Anforderungen des Bausteins OPS.2.2 *Cloud-Nutzung* berücksichtigt werden. Diese gelten sowohl bei einer Private Cloud On-Premises, wenn der Cloud-Betreiber die IT der Institution ist, als auch im Fall einer Private Cloud bei einem externen vertrauenswürdigen Cloud-Anbieter.

Wird ein externer Cloud-Anbieter für die Einrichtung einer Private Cloud genutzt, sollte sichergestellt werden, dass dieser den Sicherheitsanforderungen der Institution genügt, z. B. hinsichtlich einer durchgängigen Trennung in Netzen, Virtualisierungs-Hosts und Storage-Bereichen zwischen den Kunden des Cloud-Anbieters (Mandantentrennung). Darüber hinaus sollte abgewogen werden, ob und welche nachgelagerten Cloud-Dienste, z. B. zur Speicherung großer Datenmengen, im Rahmen der Private Cloud genutzt werden dürfen. Alle Regelungen sollten vertraglich festgelegt werden und Risiken durch Abweichungen von den Sicherheitsanforderungen müssen durch geeignete Sicherheitsmaßnahmen, z. B. Ablage ausschließlich von verschlüsselten Daten, behandelt werden.

Außerdem sollte bei der Nutzung einer Private Cloud bei einem vertrauenswürdigen Cloud-Anbieter der Grad der Abhängigkeit von diesem Anbieter berücksichtigt werden. Es sollte dokumentiert werden, was bei einem Wechsel des Anbieters bedacht werden muss. Hier kann es z. B. sein, dass beim Wechsel des Cloud-Anbieters auch neue Systeme für die TGA beschafft werden müssen.

Grundsätzlich sollte eine umfassende Analyse der Abhängigkeiten von der Cloud-Anbindung durchgeführt werden und auf Basis dieser Analyse zwischen Private Cloud On-Premises, Private Cloud bei einem vertrauenswürdigen Cloud-Anbieter oder einem Verzicht auf eine Cloud-Nutzung entschieden werden.

INF.13.M28 Sichere Nutzung von Künstlicher Intelligenz im TGM (H)

Schon bevor eine Künstliche Intelligenz (KI) als Bestandteil einer TGM-Lösung oder als eigenständiges Produkt beschafft wird, sollte beispielsweise geprüft werden, wie der Hersteller mit den gesammelten Daten umgeht, ob ein Schwachstellenmanagement besteht oder ob regelmäßige KI-spezifische Tests durchgeführt werden. Diese Anforderungen können in einer Anforderungsanalyse festgehalten werden und somit kann der geeignetste Hersteller gewählt werden. Hierbei sollte ein entsprechender Abnahmetest sicherstellen, dass die geforderten Anforderungen tatsächlich erfüllt sind. Hierzu sollte insbesondere auch INF.13.M22 *Durchführung von Systemtests im TGM* beachtet werden.

Eine sichere Nutzung von KI ist zudem sehr wichtig, da sie meist sensible Daten verarbeitet und ein aktiver Prozessbestandteil ist. Insbesondere wenn die KI für Predictive Maintenance genutzt wird, werden viele Ereignis- und Protokollierungsdaten weitergegeben.

Für eine sichere Nutzung von KI sollte insbesondere das Dokument *Sicherer, robuster und nachvollziehbarer Einsatz von KI* [BSI KI] des BSI berücksichtigt werden. Hier wird neben den klassischen Maßnahmen für Software- und Systemsicherheit dazu geraten, die KI in ein Risikomanagement einzubinden, um Mitigationsmaßnahmen ergreifen zu können. Details hierzu sind in referenziertem Dokument [BSI KI] aufgezeigt. Darüber hinaus sollte die KI in eine Protokollierung eingebunden werden, um Anomalien und Angriffe zu detektieren.

Die KI sollte in das Schwachstellenmanagement und in Penetrationstests eingebunden werden, um zu prüfen, wie sich die KI bei falschem Input oder unter Last verhält. Hierzu sollten insbesondere INF.13.M23 *Integration des TGM in das Schwachstellenmanagement* und INF.13.M30 *Durchführung von Penetrationstests im TGM* beachtet werden.

Darüber hinaus ist es wichtig, insbesondere bei der Einbindung von weiteren externen Diensten (Wetterdaten etc.), auch diese Schnittstellen auf ihre Absicherung und Zuverlässigkeit zu testen.

Auch die Plattform, auf welcher die KI bereitgestellt wird, bedarf besonderer Beachtung. Dies kann sowohl lokal, beim Hersteller oder in einer Cloud sein. Bei letzterem sollten insbesondere der Baustein OPS.2.2 *Cloud-Nutzung* sowie die Kriterien des AI Cloud Service Compliance Criteria Catalogue (AIC4) des BSI [BSI AIC4] berücksichtigt werden.

INF.13.M29 Integration des TGM in ein SIEM (H)

Eine Lösung für das Security Information and Event Management (SIEM) sammelt, analysiert und korreliert systemübergreifend Log-Einträge von Systemen und Applikationen und alarmiert bei erkannten Sicherheitsvorfällen, inklusive Angriffen. Dadurch, dass Informationen aus verschiedenen Quellen und unterschiedlichen Formaten zusammengeführt werden, können sie übersichtlich und einheitlich an einer zentralen Stelle dargestellt werden. Entscheidend ist aber, dass die gesammelten Daten system- und anwendungsübergreifend in Echtzeit analysiert und interpretiert werden, um sicherheitsrelevante Ereignisse erkennen und zeitnah auf Bedrohungen reagieren zu können.

Hierfür muss festgelegt werden, welche Protokollierungsdaten aus dem TGM an die SIEM-Lösung weitergeleitet werden. Außerdem muss die Protokollierungslösung auf Ebene des TGM eine geeignete Schnittstelle zur Anbindung an eine SIEM-Lösung unterstützen, so dass Daten im richtigen Format übergeben werden können. Diese erforderlichen Schnittstellen sollten bereits in der Anforderungsspezifikation für das TGM festgelegt werden.

In der SIEM-Lösung muss dann eine sogenannte Normalisierung der eingehenden Ereignismeldungen auf ein einheitliches (Datenbank-)Schema erfolgen, um die Ereignisse analysieren zu können. Für die eigentlichen Analysen benötigt man dann Regelwerke und geeignete Parameter. Für die speziellen Systeme der TGA und des TGM ist oft davon auszugehen, dass die SIEM-Lösung diese Systeme nicht im Auslieferungszustand unterstützt und diese Regelwerke und deren Parametrierung erst entwickelt werden müssen. Dieser Aufwand sollte möglichst frühzeitig in der Planung der SIEM-Integration berücksichtigt werden.

INF.13.M30 Durchführung von Penetrationstests im TGM (H)

Für die Durchführung von Penetrationstests im TGM sollte ein Konzept erstellt werden, das neben den verwendeten Testmethoden auch die abgestimmte Testtiefe und die Erfolgskriterien dokumentiert. Auch Notfallmaßnahmen sollten abgestimmt werden, um im Falle eines unerwarteten Ereignisses als Resultat der Tests schnell eingreifen zu können. Insbesondere die Tests sollten in diesem Konzept klassifiziert und dokumentiert werden, um die gefundenen Sicherheitslücken geeignet nachhalten und beheben zu können.

Vor allem müssen ein entsprechendes Sicherheitskonzept oder mindestens Sicherheitsrichtlinien bestehen, gegen welche getestet werden kann. Besteht ein solches nicht, ist es kaum möglich zu definieren, was tatsächlich angestrebte Ziele des Penetrationstests sind.

Falls Penetrationstests in der Produktivumgebung durchgeführt werden, muss für die betroffenen Systeme die erlaubte Testtiefe spezifiziert werden. Ansonsten kann der Ausfall eines Produktivsystems aufgrund nicht abgestimmter Penetrationstechniken oder nicht kommunizierter Risiken der

eingesetzten Techniken Regressforderungen auslösen. Im TGM kann es hier zu besonderer Schwere kommen, da eine Fehlfunktion Gefahr für Leib und Leben bedeuten kann. Dementsprechend sollten die getroffenen Regelungen in einem Vertrag festgehalten werden.

Sollte ein KI-System eingesetzt werden, muss auch dieses in den Penetrationstests mittels Negativ-Tests geprüft werden, um sicherzustellen, dass es auch beispielsweise bei bewusst manipulierten Daten, die zielgerichtet die KI zu Fehlentscheidungen bringen sollen, zuverlässig funktioniert.

3. Weiterführende Informationen

3.1. Genutzte TGM-spezifische Fachbegriffe

Automationsebene

Die Automationsebene befindet sich in der Automatisierungspyramide zwischen der Feldebene und der Managementebene. Sie führt die von der Feldebene gelieferten Daten sowie die von der Managementebene übermittelten Vorgaben zusammen. Hier erfolgt die Steuerung und Regelung der TGA-Anlagen, aber auch die Überwachung von Grenzwerten, Schaltzuständen oder Zählerständen.

Building Information Modeling (BIM)

Gemäß VDI 2552 Blatt 2 ist BIM eine Methodik zur Planung, zur Ausführung und zum Betrieb von Bauwerken mit einem kollaborativen Ansatz auf Grundlage eines digitalen Informationsmodells des Bauwerks zur gemeinschaftlichen Nutzung.

Computer-Aided Facility Management (CAFM)

Gemäß VDI 3814 Blatt 2.1 dient CAFM als Werkzeug zur Erfassung, Verarbeitung, Aufbereitung und Archivierung von Daten und Informationen mit dem Ziel, die Leistungsprozesse und Aufgaben in der Betriebsphase eines Gebäudes zu unterstützen.

Feldebene

Die Feldebene stellt die unterste Ebene der Automatisierungspyramide dar und umfasst unterschiedliche Komponenten der GA oder OT. In der Regel werden hier Sensoren und Aktoren betrieben. Sensoren erfassen Informationen (z. B. Bewegung, Helligkeit, Temperatur) und senden diese an die Automationsebene. Aktoren empfangen Steuerinformationen und setzen diese in Schaltsignale um, z. B. für die Beleuchtungs-, Heizungs-, Klima- und Lüftungsanlage.

Gebäude

Der Begriff Gebäude wird im Baustein INF.13 *Technisches Gebäudemanagement* und in diesen zugehörigen Umsetzungshinweisen synonym für Gebäude, Gebäudekomplex, Liegenschaft und Liegenschaftsportfolio genutzt. Außerdem beschreibt der Begriff Gebäude nicht nur Häuser und Hallen, sondern auch beispielsweise einen Fernsehturm oder eine Bohrinsel.

Gebäudeautomation (englisch Building Automation and Control Systems, BACS)

Die Gebäudeautomation (GA) umfasst gemäß VDI 3814-1 alle Produkte und Dienstleistungen zum zielsetzungsgerichteten Betrieb der Technischen Gebäudeausrüstung.

Gebäudekomplex

Ein Gebäudekomplex ist eine Gruppe von Gebäuden, die baulich miteinander verbunden sind und als Gesamteinheit wahrgenommen werden.

Gewerk

Im Bauwesen umfasst ein Gewerk im Allgemeinen die Arbeiten, die einem in sich geschlossenen Bauleistungsbereich zuzuordnen sind. Es handelt sich um einen Funktionsbereich, der insbesondere verschiedene TGA-Anlagen umfassen kann.

Beispiel: Raumlufttechnische Anlagen (Kostengruppe 430 in DIN 276), wozu etwa Lüftungsanlagen, Klimaanlagen und Kälteanlagen gehören.

Leitstand (englisch Control Center)

Ein Leitstand (auch Bedien- und Beobachtungseinheiten) ist ein technisches Werkzeug zur Visualisierung aktueller Abläufe, Zustände und Situationen von Prozessen, inklusive TGM- und speziell GA-Prozesse.

Liegenschaft

Eine Liegenschaft ist ein Grundstück inklusive seiner Bebauung. Zur Bebauung gehören alle unbeweglichen Sachen, d. h. Gebäude und sonstige Dinge, die nicht ohne Weiteres vom Grundstück entfernt werden können.

Liegenschaftsportfolio

Als Liegenschaftsportfolio wird die Gesamtheit der Liegenschaften im Besitzstand bezeichnet.

Nachfrageorganisation

Eine Nachfrageorganisation ist gemäß DIN EN ISO 41011 eine Organisationseinheit innerhalb oder außerhalb der Institution, die für ihre Erfordernisse autorisiert ist, entsprechende Anforderungen an TGA, GA oder TGM zu stellen und die Kosten zur Erfüllung der Anforderungen zu übernehmen.

Beispiele: Mieter innerhalb eines Gebäudes, Eigentümer eines Gebäudes, Dienstleister innerhalb einer Institution, z. B. Kantine.

System

Der Begriff System adressiert im Baustein INF.13 *Technisches Gebäudemanagement* und in diesen zugehörigen Umsetzungshinweisen nicht nur ein IT-System im klassischen Sinn (vgl. Bausteine der Schicht SYS), sondern umfasst auch alle Komponenten der TGA einschließlich aller Komponenten der Feldebene, wie Sensoren, Aktoren usw.

Technische Gebäudeausrüstung (englisch Building Services, BS)

Die Technische Gebäudeausrüstung (TGA) umfasst gemäß VDI 4700 Blatt 1 alle im Bauwerk eingebauten und damit verbundenen technischen Einrichtungen und nutzungsspezifischen Einrichtungen sowie technische Einrichtungen in Außenanlagen und Ausstattungen. Gewisse Komponenten der Gebäudeautomation sind ebenfalls zur TGA zuzurechnen, z. B. echtzeitfähige Industrial Ethernet Switches.

Technisches Gebäudemanagement (englisch Technical Building Management, TBM)

Das Technische Gebäudemanagement (TGM) beinhaltet gemäß DIN 32736 alle Leistungen, die zum Erhalt der technischen Funktion und Verfügbarkeit eines Gebäudes dienen. Das TGM übernimmt somit für die TGA das Betreiben, Instandhalten, Modernisieren und Dokumentieren der Komponenten und definiert alle notwendigen Prozesse.

TGA-Anlage

Eine Anlage der TGA beschreibt die Gesamtheit aller zur Erfüllung bestimmter Funktionen zusammenwirkenden technischen Komponenten. Beispiele gemäß DIN 276 „Kosten im Bauwesen“ sind Wärmeversorgungsanlagen, Lüftungsanlagen oder Beleuchtungsanlagen.

3.2. Abkürzungen

Abkürzung	Bedeutung
5G	5. Generation des Mobilfunks
BACS	Building Automation and Control Systems
BBR	Bundesamt für Bauwesen und Raumordnung
BIM	Building Information Modelling

Abkürzung	Bedeutung
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
BS	Building Services
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAFM	Computer-Aided Facility Management
CLI	Command Line Interface
DDC	Direct Digital Controller
DIN	Deutsches Institut für Normung
GA	Gebäudeautomation
GU	Generalunternehmer
ISMS	Information Security Management System
ISO	Internationale Organisation für Normung
IT	Informationstechnik
KI	Künstliche Intelligenz
LTE	Long Term Evolution
NAC	Network Access Control
NEA	Netzersatzanlage
OT	Operational Technology
RLT	Raumlufttechnik
RZ	Rechenzentrum
SIEM	Security Information and Event Management
TBM	Technical Building Management
TFTP	Trivial File Transfer Protocol
TGA	Technische Gebäudeausrüstung
TGM	Technisches Gebäudemanagement
TÜV	Technischer Überwachungsverein
USV	Unterbrechungsfreie Stromversorgung
VDI	Verein Deutscher Ingenieure e.V.

3.3. Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.4. Quellenverweise

[BSI AIC4] BSI, „AI Cloud Service Compliance Criteria Catalogue (AIC4)“, Februar 2021, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/AIC4/AI-Cloud-Service-Compliance-Criteria-Catalogue_AIC4.html, zuletzt abgerufen am 24.08.2021

[BSI KI] BSI, „Sicherer, robuster und nachvollziehbarer Einsatz von KI“, Februar 2021, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Herausforderungen_und_Massnahmen_KI.pdf, zuletzt abgerufen am 24.08.2021

[BSI C5] BSI, Cloud Computing Criteria Catalogue, Oktober 2020, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf, zuletzt abgerufen am 24.08.2021