White Paper GEFMA 944

Cybersicherheit im Facility Management

Autor: gefma-Arbeitskreis Digitalisierung
Veröffentlicht durch: gefma

Version: 1.0/2025-10

Inhalt

1	**Motivation und Zielsetzung**	**3**
2	**Pommes mit Chlor – eine tragische Geschichte**	**6**
3	**Grundlagen**	**7**
3.1	Cybersicherheit im Facility Management	7
3.2	Ausgangssituation	8
3.3	Konsequenzen für das Immobilien- und Facility Management	12
3.4	Prozessuale, operative und betriebliche Aspekte	14
3.5	Rechtliche Grundlagen, Normen, Richtlinien und Zertifizierungen	15
4	**Mögliche Einfallstore, Anwendungen und Risiken**	**26**
4.1	Cyberangriffe auf Aufzüge	26
5	**Wesentliche Maßnahmen**	**29**
5.1	Technische Maßnahmen	31
5.2	ICS-Monitoring (Industrial Control System Security)	33
5.3	Überprüfung der Maßnahmen	34
5.4	Erforderliche Rollen und Prozesse (Aufbau-/ Ablauforganisation)	35
6	**Fazit**	**37**
7	**Literaturverzeichnis**	**38**
8	**Abbildungs- und Tabellenverzeichnis**	**40**
	Impressum	41

1 Motivation und Zielsetzung

„Alles was nötig war, war ein Holzstock!“ — diese saloppe Aussage war überraschend. Sie waren gerade innerhalb von knapp 20 Minuten in ein gesichertes Rechenzentrum in Frankfurt am Main eingebrochen. Wie war das möglich? Der Tathergang: morgens halb 10 in Deutschland, drei Personen in normaler Arbeitskleidung, Blaumann, Bosch-Hose und Elektriker-Jacke an der Eingangstür zur Tiefgarage. Diskutierend. Die Tiefgarage wurde von einem prominenten Rechenzentrum in Frankfurt am Main mitgenutzt, die Kunden, die dort ein- und ausgingen, um ihre Daten und Server dort zu platzieren, waren Banken und Versicherungen. Die Menschen, die dort gerade diskutierten, waren Profis. Nur keine Elektriker oder Mechaniker, sondern Hacker, die den Auftrag hatten, dort unbemerkt einzubrechen und Daten zu entwenden.
Nach ca. dreißig Sekunden hob einer der Diskutanten einen Holzstock vom Gehsteig auf, steckte ihn durch das Gittertor der Tiefgarage, drückte einen Knopf auf der anderen Seite des Tores. Das Tor fuhr hoch – die Drei gingen entspannt in das Gebäude. In der Tiefgarage gab es neben zahlreichen Zutrittsschranken auch Notfallschalter. Diese Schalter waren via RJ54 angebunden (oranges Verlegekabel). Also: Schalter aufschrauben, Kabel herausnehmen, Stecker ankrimpen und einstecken in den mitgebrachten Laptop. Jetzt noch schnell die 192.168.0.2 aufrufen, die SSSiedle Steuerungsanlage mit „admin:admin123!“ öffnen — der Techniker vor Ort hat dankenswerterweise das Standardherstellerpasswort nicht geändert. Nun noch alle Türen auswählen und „Öffnen“ drücken. Auftrag beendet. Der Auftraggeber war nicht wirklich glücklich. Dies war der achte Weg in das Rechenzentrum, den das Team an diesem Tag gefunden hatte.

Dem Facility Management (FM) kommt bei der Vereitelung von Attacken eine erhebliche Bedeutung zu. Neben der Sicherung der Gebäudezugänge ist auch der Schutz der Zugänglichkeit über die IT-Infrastruktur durch das FM notwendig.
Angriffe auf Systeme der Gebäudeautomation oder Brandmeldeanlagen können Gefahr für Leib und Leben nach sich ziehen, wenn z. B. Meldeanlagen manipuliert werden, die für die Gefahrenabwehr notwendig sind. Im Zuge der fortschreitenden Vernetzung dieser Systeme mit der klassischen Informationstechnik reichen Angriffe potenziell bis tief in die Unternehmens-IT und können Datenverlust, -verschlüsselung und Sabotageakte zur Folge haben.

Die intensive Vernetzung der Softwareanwendungen im FM mit Elementen der Gebäudeautomation (GA) ermöglicht neue, effizientere Arbeitsprozesse wie die gebrauchsgerechte, automatische Steuerung von Heizung und Lüftung entsprechend der in der Anwendungssoftware geplanten Raumnutzung. Daten aus der GA und der Gebäudeleittechnik (GLT) werden für Anwendungen verfügbar und ermöglichen so die vorausschauende Wartung von technischen Anlagen und die Optimierung des Energieverbrauchs.
Die Gebäudeautomation und -steuerung bieten vermehrt Funktionen zur Vernetzung mit Internetdiensten. IoT (Internet of Things) -Geräte kommunizieren mit Cloud-Diensten und Komponenten wie Sicherheitskameras und Photovoltaikanlagen verfügen über GSM (Global System for Mobile Communications) -Module, die eine direkte Verbindung zum Internet ermöglichen.

Mit der fortschreitenden Digitalisierung wird moderne Sicherheits- und Gebäudeleittechnik mit Softwareanwendungen über Kommunikationsprotokolle und -wege der klassischen IT wie Webservice, Datenbankzugriffe oder http-Requests verbunden. Neben der Steuerungstechnik sind auch die Aktoren und Sensoren über diese Protokolle in die Netzwerkstrukturen eingebunden.

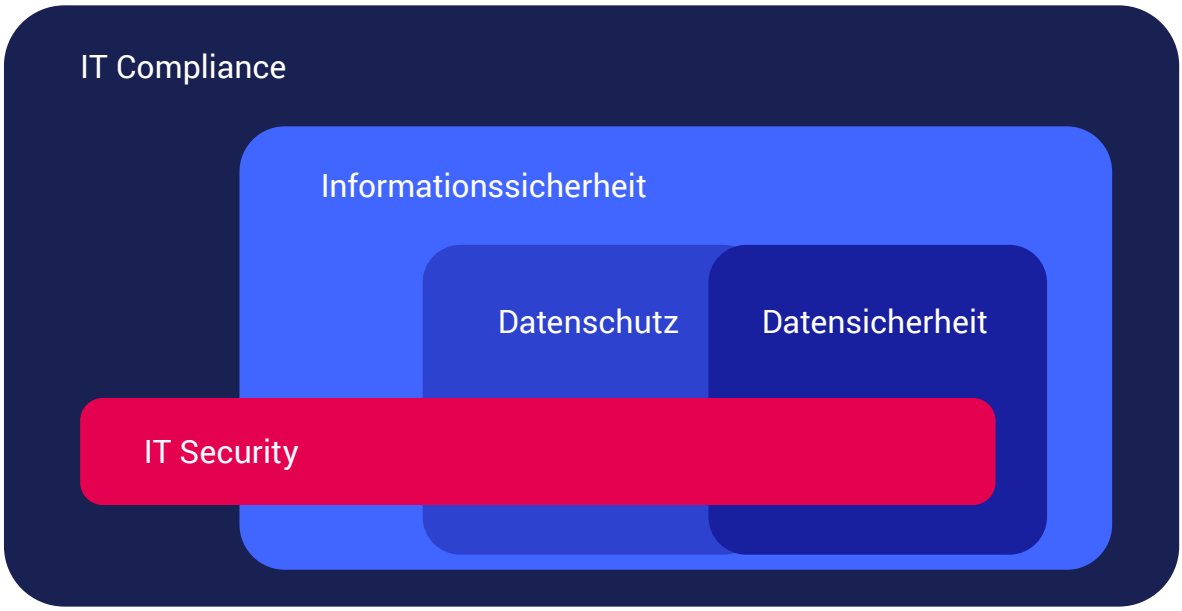
Mit den „Technischen Regeln für Betriebssicherheit [TRBS 1115-1 Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (MSR)]“ wird die Beschäftigung mit Cybersicherheit zu einem Teil der gesetzlichen Betreiberpflichten.

Dabei bezieht sich die TRBS 1115-1 nur auf sicherheitsrelevante MSR.
Die möglichen Einfallstore für Cyberattacken befinden sich allerdings in der gesamten GLT und GA.

Neben der Absicherung der einzelnen Komponenten gegen unerlaubten Zugriff (sog. Rollen- und Rechtemanagement) sind die Organisation der Netzwerkstrukturen und die Absicherung der Kommunikationswege und -arten wichtige Maßnahmen zur Erhöhung des Sicherheitsniveaus. Der Betrieb von IoT-Geräten, die über Internetverbindungen von zentralen Administrationsplattformen gesteuert werden, stellt den Betreiber vor weitere Herausforderungen.
Die Verantwortung für diese Systeme muss klar geregelt und dokumentiert werden. Eine Delegation kann nur dann erfolgen, wenn auch geeignete Maßnahmen zur Kontrolle eingesetzt werden und effektiv sind.

Im produzierenden Gewerbe kommt der Sicherheit der sog. Operational Technology (OT) — also der IT-Sicherheit in der Produktionstechnik — erhöhte Aufmerksamkeit zu. Es werden spezielle Monitoring-Verfahren eingesetzt, die ein Eindringen von außen in die Netze und Komponenten erkennen und geeignete Maßnahmen dagegen auslösen.
Diverse IT-Dienstleister bieten auf OT-Sicherheit spezialisierte Beratungsleistungen an. Sie analysieren Netzwerkstrukturen und -komponenten und unterstützen beim Aufbau einer sicheren Architektur, der darauf fußenden Infrastruktur und der Implementierung entsprechender Monitoring-Lösungen (Industrial Control System (ICS) Monitoring).
Diese Verfahren sind auch für das Facility Management anwendbar.

Abbildung 1: Zusammenhang der Begriffe der Informationssicherheit[1]



[1] Kevin Wennemuth, CID GmbH, 2024

Die Cybersicherheit, im Fachjargon oft IT-Sicherheit genannt, steht im Kontext ihrer Wirksamkeit nicht allein. Die ist eingebettet in weitere Wirkungsdomänen, wie Datensicherheit und Datenschutz. Die IT-Sicherheit verfolgt im Wesentlichen die Sicherstellung des technischen Schutzes von IT-Infrastrukturen. Hierzu gehören sowohl technische Geräte und Software als auch Prozesse und gefährdete Menschen.

Während Datensicherheit alle Maßnahmen zur Sicherung von Daten jeglicher Art umfasst, widmet sich der Bereich Datenschutz den gesetzlichen Pflichten zum Schutz personenbezogener Daten.

Die Informationssicherheit wiederum fasst diese Bereiche zusammen und bildet mit ihren Regularien und Anweisungen die zusammenführende Klammer der Themen. Ihr Hauptaugenmerk ist die Sicherstellung der Schutzziele von Vertraulichkeit von Daten, der Verfügbarkeit von Daten und Systemen und die Integrität von Informationen.

Die in diesem White Paper angesprochenen Themen und komplexen Situationen tangieren alle hier aufgezeigten Domänen.

2 Pommes mit Chlor – eine tragische Geschichte

Schwimmbäder sind etwas ganz Besonderes. Wer kennt sie nicht, die Mischung aus Pommesduft und Chlorgeruch gepaart mit Kindergeschrei — ein typisches Schwimmbad im Sommer. Aber was hat das mit Cybersicherheit zu tun, möge man sich fragen? Der übermäßige Konsum von Pommes hat bekanntermaßen nur selten direkt lebensbedrohliche Konsequenzen. Der übermäßige „Konsum“ von Chlor allerdings sehr wohl. „Aber Chlor isst doch niemand freiwillig!“. Das stimmt, nur leider obliegt die Konzentration des Chlors im Wasser der Leitung des Schwimmbades, genauer gesagt der Steuerungsanlage mit verbauter Speicherprogrammierbarer Steuerung (SPS) S7 von Siemens. Und weil es einfach ist, kann die Anlage natürlich auch von der Leitwarte aus gesteuert werden, die 20 km entfernt ist. Dem Internet sei Dank! Die Anlage ist, wie viele andere Anlagen auch, aus dem Internet erreichbar — ein Wunderwerk der Technik! Auf strenge Sicherheitsvorschriften wurde natürlich geachtet — alle notwendigen Excel-Formulare, die die Sicherheit herstellen sollten, wurden ausgefüllt. Der ISB hat alle Dokumente zur Zufriedenheit geprüft. Von einer technischen Sicherung wurde deswegen abgesehen. Was sollte schon schiefgehen? Ein Schwimmbad ist doch keine Bedrohung!

Ja, was soll schon schiefgehen an einem Samstagnachmittag mit 2.000 Besuchern? Man wird sich später erzählen, dass Menschen mit Verbrennungen dritten Grades auf dem Parkplatz lagen und nicht genügend Hilfskräfte vor Ort waren, um alle zu versorgen. Überall hörte man Menschen schreien und Kinder weinen. Ein tragischer Tag für viele. Was war geschehen?

Einem Angreifer aus dem Internet war es gelungen durch das Ausnutzen von bekannten bzw. schwachen Passwörtern und fehlenden sonstigen Sicherheitsmaßnahmen auf die Steuerungsanlage des Schwimmbades zuzugreifen. Die Steuerung selbst ist einfach, ein paar Pfeile drücken, Mengen auf Maximum einstellen und „Release“ drücken. Das verstehen sogar Laien schnell. Und schon wurde die komplette Jahresdosis Chlor in das große Becken entlassen. Die Schwimmenden verbrannten sich quasi im Wasser, während die Umgebung des Beckens mit sich schlagartig bildendem Chlorgas geflutet wurde. Der Rest ist bekannt.

3 Grundlagen

3.1 Cybersicherheit im Facility Management

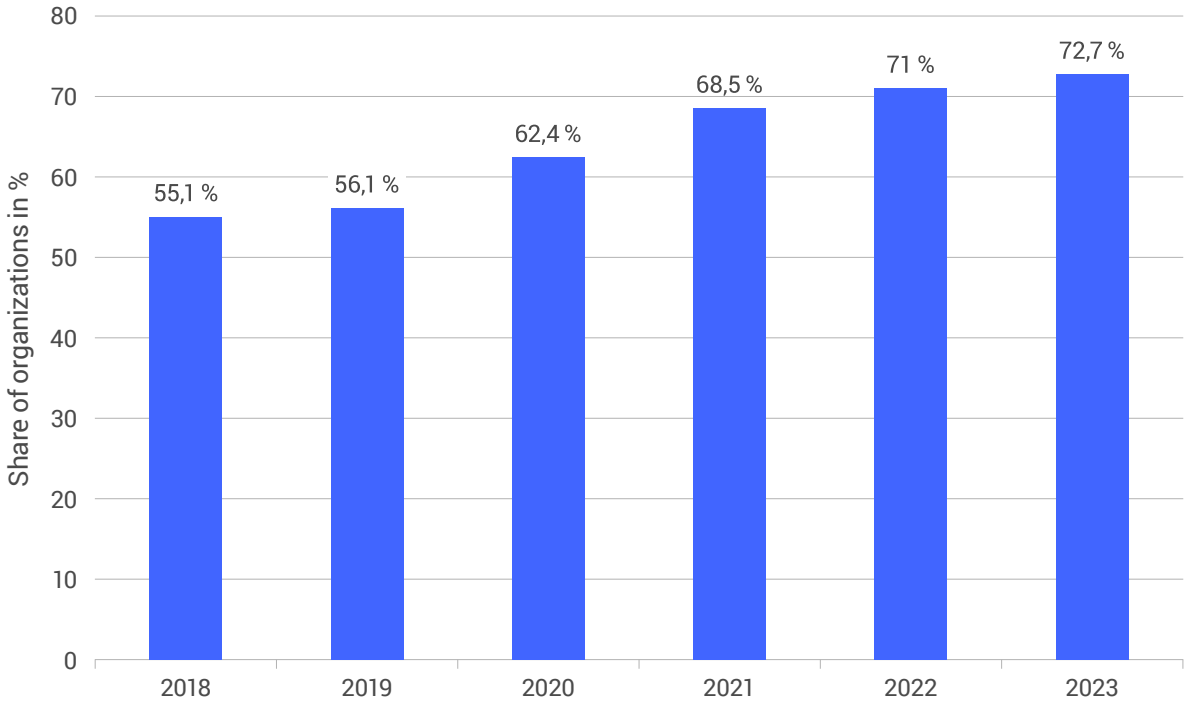
IT-Sicherheit im Facility Management ist der Schutz von Werten im Unternehmen im Kontext von FM. Dies kann Hard- und Software sowie Daten, aber auch Prozesse, Intellectual Property (IP) oder Menschen und deren Verhalten beinhalten.
Sie beinhaltet Strategien und Methoden, die implementiert werden, um digitale Systeme, Netzwerke und Daten, die im Zusammenhang mit dem Management von Gebäuden und Anlagen stehen, vor Cyberbedrohungen zu schützen. Auch der Schutz von Gebäudeautomatisierungssystemen, Sicherheitssystemen, Kommunikationssystemen und anderen Technologien, die für den Betrieb von Facilities verwendet werden, stehen hier im Fokus.
Sie umfasst die Identifizierung potenzieller Schwachstellen, die Implementierung von Sicherheitsprotokollen und -maßnahmen, die Überwachung von Systemen bzgl. Anomalien, die Reaktion auf Sicherheitsvorfälle und die Wiederherstellung von Systemen nach einem Angriff. Ziel ist es, die Integrität, Verfügbarkeit und Vertraulichkeit der Systeme und Daten im FM zu gewährleisten. Sie ist ein wesentlicher Aspekt des Risikomanagements in der modernen Gebäudeverwaltung.

3.2 Ausgangssituation

In den letzten Jahren hat sich die Welt des Immobilien- und Facility-Managements tiefgreifend verändert. Digitale Technologien und vernetzte Systeme sind aus modernen Gebäuden nicht mehr wegzudenken. Smarte Heizungs-, Lüftungs- und Klimaanlagen (HLK), Zutrittskontrollsysteme, Aufzüge und Beleuchtungssteuerungen sind nur einige Beispiele für Anwendungen, die heute über das Internet gesteuert und überwacht werden. Diese Entwicklungen bieten einerseits erhebliche Effizienz- und Komfortgewinne, eröffnen jedoch andererseits auch neue Angriffsflächen für Cyberkriminelle.

Derzeitige Statistiken sprechen für sich. Die Frequenz von weltweiten Cyberangriffen steigt jedes Jahr um 15–20 %. Bereits für das Jahr 2025 rechnet man weltweit mit einem Schaden von 10.5 Billionen EUR durch Cyberangriffe. Global gesehen sind im Jahr 2023 bereits 72,7 % aller Unternehmen Opfer einer erfolgreichen Cyberattacke geworden.

Abbildung 2: Übersicht weltweiter Cyberangriffe pro Jahr[2]



[2] „www.statista.com“, 15.01.2025 [Online]. Available: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

Statistisch gesehen wird jeder einmal Opfer von Cyberattacken. Der durchschnittliche Schaden einer erfolgreichen Cyberattacke liegt hierbei im Durchschnitt bei 4,5 Mio. EUR. Eine Erpressung ist das wahrscheinlichste Angriffsszenario. Die IT-Infrastrukturen werden gekapert und verschlüsselt und das Opfer wird zur Zahlung von beträchtlichen Summen erpresst.

Das BSI stellt hinsichtlich der Gefährdungslage im Technischen Gebäudemanagement folgende Schwachstellen fest:

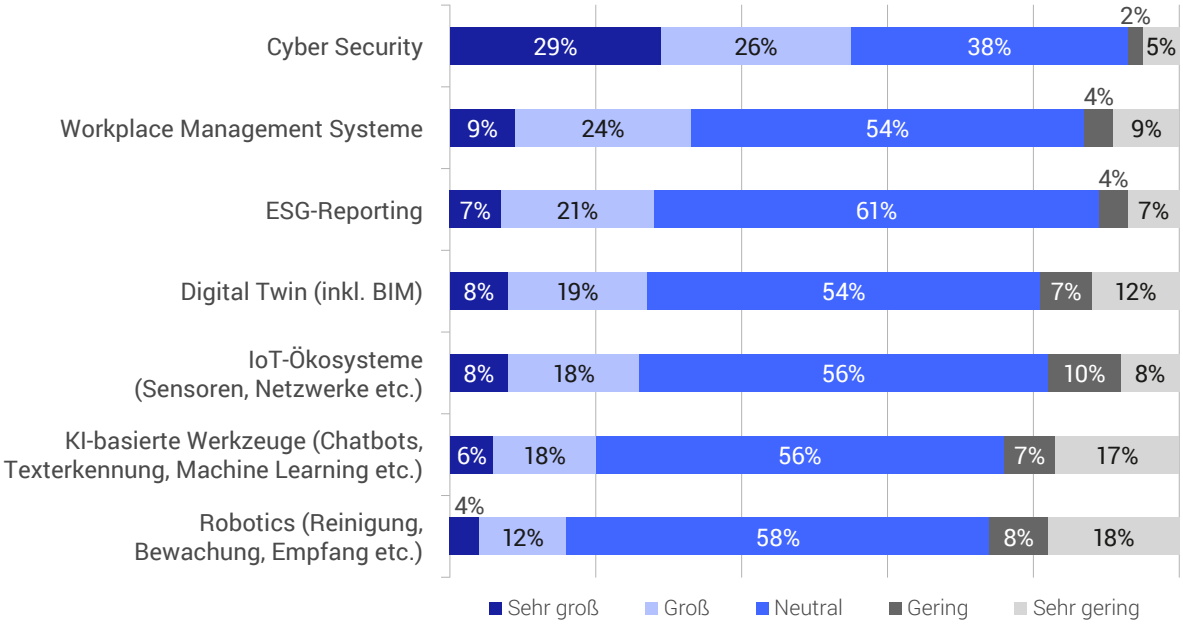
- Fehlende Grundlagen für die Planung des TGM vor der Nutzungsphase
- Mangelnde Dokumentation des Technischen Gebäudemanagements (TGM) bei der Übergabe an den Nutzer
- Die Kompromittierung der Schnittstellen zwischen TGM und Anlagen kann zu Fehlfunktionen führen oder Sabotageakte begünstigen
- Die TGA und GA werden unzureichend durch ein entsprechendes Monitoring überwacht
- Das Rollen- und Berechtigungsmanagement werden unzureichend umgesetzt und aktualisiert

Wenn wir uns die Trends der letzten Digitalisierungsstudie der gefma & Lündendonk [3] ansehen, stehen viele technologische Ansätze ganz oben auf der Agenda, die von der Vernetzung und Integration zahlreicher unterschiedlicher Anwendungen abhängig sind. Diese Anwendungen werden in der Regel und zukünftig noch stärker Cloud-basiert betrieben und mit offenen APIs verbunden. Im Bereich der IoT-Anwendungen werden auch weitere externe Datenquellen wie z. B. Wetterprognosen immer relevanter.

Die Bewirtschaftung und Entwicklung von Gebäuden erfordert die Zusammenarbeit von Facility Managern mit externen Dienstleistern und Subunternehmern. Diese komplexe Struktur macht eine klare Regelung der Zuständigkeiten für die Sicherheit in der Gebäudeautomation unverzichtbar. Verantwortlichkeiten müssen klar definiert und vertraglich festgelegt werden, um Sicherheitslücken und Missverständnisse zu vermeiden. Die Anwenderseite hat diese Risiken bereits erkannt. Dementsprechend ist es auch nachvollziehbar, dass die Anwenderseite gemäß der gefma & Lünendonk[3] Studie mit Abstand am meisten Budget für das Thema Cybersicherheit einplant.

[3] g. &. Lünendonk, GEFMA 945: CAFM-/IWMS-Trendreport 2023, 2023

Abbildung 3: Aktuelle Herausforderungen für die Budgetplanung der Anwender[3]



Früher galt IT-Sicherheit als rein technische Herausforderung für die IT-Abteilung. Heute ist sie eine essenzielle Managementaufgabe, die alle Verantwortlichen im Immobilien- und Facility Management betrifft. Angriffe auf digitale Systeme können nicht nur den IT-Betrieb stören, sondern auch physische Schäden verursachen, den Zugang zu Gebäuden verhindern oder kritische Infrastrukturen lahmlegen. Die Bedrohung reicht von Datendiebstahl und Industriespionage bis hin zu Sabotage und Erpressung durch Ransomware (Software zur Verschlüsselung von Daten).

Ein weiterer Treiber dieser Entwicklung ist die zunehmende Vernetzung von IT-Systemen der Gebäudeautomation und -leittechnik mit der klassischen IT und die Integration von Cloud-Diensten. Daten aus Gebäude- und Energiemanagementsystemen werden in Echtzeit gesammelt, ausgewertet und zur Optimierung genutzt. Dies erhöht jedoch auch die Anforderungen an sichere IT-Strukturen und an den Schutz sensibler Daten.

[3] g. &. Lünendonk, GEFMA 945: CAFM-/IWMS-Trendreport 2023, 2023

Für Facility- und Immobilienmanager bedeutet das, dass Cybersicherheit zu einem unverzichtbaren Teil ihrer Verantwortung wird. Sie müssen verstehen, welche Systeme vernetzt sind, welche Daten verarbeitet werden und welche Risiken bestehen. Präventive Maßnahmen wie regelmäßige Sicherheitsüberprüfungen, Schulungen für Mitarbeitende und die Zusammenarbeit mit IT-Experten sind unverzichtbar, um Gebäude sicher und betriebsfähig zu halten.

Die zunehmende Digitalisierung ist eine Chance und gleichzeitig eine Herausforderung. Wer die Risiken ernst nimmt und frühzeitig Schutzmaßnahmen ergreift, sichert nicht nur die eigene Wettbewerbsfähigkeit, sondern schützt auch die Werte, die ihm anvertraut sind.

3.3 Konsequenzen für das Immobilien- und Facility Management

Auf alle Akteure am Immobilienmarkt mit seinen vielfältigen Ausprägungen und Aufgaben kommen neue Herausforderungen und damit auch Chancen zu. Ob Bauherr, Nutzer, Eigentümer oder Verwalter – die neuen Richtlinien und Gesetze zum Thema Cyberresilienz (=Widerstandsfähigkeit von IT-System gegen Cybercrime) betreffen alle. Dies erfordert vor allem eine wichtige und zielgerichtete Kommunikation und Abstimmung zwischen den Marktakteuren. Insbesondere im Phasenübergang zwischen Bau und Betrieb wird diese Kommunikation notwendig. Eine gute Dokumentation und stringente Umsetzung der Vorgaben und Best Practices bereits in der Planung sind essenziell. Hier sollten Themen wie Datenspeicherung, Cloud-Nutzung oder Smart-Metering/BIM erörtert und strategisch betrachtet werden.

Die EU-Richtlinien zum Digital Operational Resilience Act (DORA) treffen derzeit den Banken- und Versicherungssektor und damit natürlich auch die IT-Betreiber und Zubringer dort.[4] In DORA werden umfangreiche und praktisch belastbare Nachweise einer digitalen Resilienz gegen Cyberangriffe (auch physikalisch hybrid) gefordert. Die Bundesanstalt für Finanzdienstleistungsaufsicht (Bafin) beschreibt auch das Vorgehen im Rahmen von hybriden Angriffseinsätzen (sog. Red Teaming) in Form des TIBER-DE.[5]

Momentan erst den Finanzsektor betreffend, geht die IT-Branche davon aus, dass dieses Regelwerk auch in anderen kritischen Sektoren (z. B. KRITIS, Telekommunikation) adaptiert wird. Der EU-Rechtsakt zur Cyberresilienz[6] geht bereits im Verbrauchermarkt in diese Richtung. Auch wenn die CRA vorrangig Verbrauchsgegenstände einbezieht, sind hier ebenfalls Smart-Building-Geräte mit betroffen. Von Sensorik über SPS-Anlagen bis hin zu Telemetrie ist hier nichts ausgeschlossen.

Auch die Richtlinie zur Definition von Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Europäischen Union[7] zielt in diese Richtung. Neben Anforderungen an Mindeststandards enthält diese Richtlinie auch Haftungsregeln im Falle einer fahrlässigen Handlung, also dem absichtlichen Weglassen von Sicherungsmaßnahmen, obwohl diese angezeigt wären.

Basierend auf dem europäischen Rechtsakt zur Cybersicherheit (Cybersecurity Act) hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland bereits 2019 angefangen, die einschlägigen Anforderungen und Gesetze in IT-Sprache zu übersetzen. Der BSI IT Grundschutz-Katalog[8] definiert hierbei

[4] „Digital Operational Resilience Act (DORA)“, 15.01.2025 [Online]. Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[5] „TIBER-DE“, 07.02.2025. [Online]. Available: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/tiber-de/tiber-de-816986

[6] „Eu Cyber Security Act“, 15.01.2025 [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/Cyber-Security-Act/cyber-security-act.html

[7] „NIS2-Richtlinie“, 15.01.2025 [Online]. Available: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148

[8] „BSI-Grundschutzkataloge“, 15 01 2025. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.htm

ein umfangreiches und auch hybrid gestaltetes Rahmenwerk zum Abgleich der eigenen Cyberresilienz. Dieser Grundschutz zählt in der IT-Branche mittlerweile zum Mindeststandard in Bereichen wie KRITIS, Manufacturing und IT.

Alle diese Richtlinien und Gesetze sehen keine Karenzzeit vor, werden oder sind also unmittelbar rechtlich bindend.

3.4 Prozessuale, operative und betriebliche Aspekte

Unternehmen sind nach dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)[9] aufgefordert „angemessene organisatorische und technische Vorkehrungen zu treffen". Innerhalb der IT-Sicherheit stellt der Bereich der OT-Sicherheit ein komplexes Teilgebiet dar.

Um den Anforderungen zur IT-Sicherheit gerecht zu werden, müssen zwischen FM- und IT-Abteilungen die Verantwortungen klar abgegrenzt aber auch eine effektive Kooperation gesichert werden. Richtlinien für den Betrieb der OT-Komponenten müssen gemeinsam erarbeitet werden.
Die Netzwerke und Komponenten der Gebäudeleit- und Gebäudeautomationstechnik sowie der Sicherheitstechnik liegen häufig in der Zuständigkeit des FM. Weitere an der Gestaltung dieser Netzwerke beteiligten Personengruppen sind externe Dienstleister und Lieferanten von Komponenten und Technologien.
Alle Akteure müssen für ihre Verantwortung hinsichtlich der IT-Sicherheit sensibilisiert werden. Werden z. B. Standardpasswörter von Komponenten nicht verändert, physische Schnittstellen von Geräten nicht gesperrt oder direkte Kommunikationswege in das Internet ermöglicht, so wird eine neu verbaute Komponente zum möglichen Einfallstor für Angreifer.

Der Facility Manager muss sich dieser Verantwortung bewusst sein und bei Bedarf Spezialisten zu Rate ziehen. Insbesondere bei Zukauf oder Anmietung von Gebäuden darf die Anbindung der GLT bzw. GA an zentrale IT-Systeme (z. B. Mailrelay, Energiemanagement) nicht ohne genaue Sicherheitsüberprüfung vor Ort ermöglicht werden.

[9] „BSIG-, BSI-, IT-Sicherheitsgesetz", 15.01.2025 [Online]. Available: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html; C5-Zertifizierung (Cloud Computing Compliance Criteria Catalogue)

3.5 Rechtliche Grundlagen, Normen, Richtlinien und Zertifizierungen

Um den in den vorangestellten Abschnitten beschriebenen Gefahren und Situationen zu begegnen, sind Unternehmen verpflichtet, eine Reihe von rechtlichen Grundlagen, Normen und Richtlinien zu beachten. Diese haben auch Auswirkungen auf das Facility Management bzw. den Gebäudebetrieb im Allgemeinen.

Diese Regularien sollen nicht nur die Sicherheit sensibler Daten und die Integrität technischer Systeme gewährleisten, sondern auch den rechtlichen Rahmen schaffen, in dem Sicherheitsvorkehrungen umgesetzt und überprüft werden müssen. Durch die Einhaltung dieser Vorgaben können Facility Manager nicht nur rechtliche Risiken minimieren, sondern auch die Verfügbarkeit und den Schutz von Gebäudemanagementsystemen gewährleisten.

Ein weiterer entscheidender Faktor ist die Zertifizierung. Unternehmen haben die Möglichkeit, durch entsprechende Zertifizierungen ihre Compliance und Sicherheitsstandards offiziell bestätigen zu lassen. Zertifizierungen wie ISO/IEC 27001 oder der C5-Katalog des BSI helfen nicht nur dabei, nachzuweisen, dass die entsprechenden Vorgaben erfüllt werden, sondern stärken auch das Vertrauen von Kunden und Partnern. Besonders für Betreiber kritischer Infrastrukturen, wie sie im Facility Management oft vorkommen, sind solche Zertifizierungen ein wichtiger Nachweis, dass Sicherheitsvorkehrungen auf höchstem Niveau umgesetzt werden.

Nachfolgend werden einige der rechtlichen Grundlagen, Normen, Richtlinien und relevanten Zertifizierungen näher beschrieben, die vor allem auf den Betrieb von Gebäuden und Immobilien einen hohen Einfluss haben.

3.5.1 Rechtliche Grundlagen

IT-Sicherheitsgesetz (IT-SiG)
Das IT-Sicherheitsgesetz richtet sich an Betreiber kritischer Infrastrukturen (KRITIS), die für die Versorgung und Sicherheit der Bevölkerung essenziell sind. Dazu zählen Sektoren wie Energie, Wasser, Gesundheit, Informationstechnik und Transport. Im Facility Management ist das Gesetz vor allem dann relevant, wenn Unternehmen Gebäude und Anlagen betreuen, die zu diesen kritischen Infrastrukturen gehören. Systeme, die zur Steuerung von Gebäuden und Anlagen eingesetzt werden, müssen daher besondere Sicherheitsanforderungen erfüllen, um die Funktionsfähigkeit sicherzustellen und Risiken zu minimieren.

Der Zweck des IT-Sicherheitsgesetzes ist es, die IT-Sicherheit in kritischen Infrastrukturen zu verbessern und die Widerstandsfähigkeit gegen Cyberangriffe zu stärken. Betreiber werden verpflichtet, technische und organisatorische Maßnahmen zum Schutz ihrer IT-Systeme zu ergreifen, Sicherheitsvorfälle zu melden und regelmäßige Audits durchzuführen. Im Facility Management soll das Gesetz sicherstellen, dass IT-Systeme, die Gebäudetechnik oder Überwachungsprozesse steuern, vor potenziellen Cyberbedrohungen geschützt sind, um die Verfügbarkeit und Integrität der Infrastruktur zu gewährleisten.[10]

[10] „IT-Sicherheitsgesetz (IT-SiG)“, 15.01.2025 [Online]. Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

Datenschutz-Grundverordnung (DSGVO)
Die Datenschutz-Grundverordnung (DSGVO) ist eine EU-weite Verordnung, die den Schutz personenbezogener Daten regelt. Sie legt fest, wie Unternehmen und Organisationen personenbezogene Daten sammeln, verarbeiten, speichern und weitergeben dürfen. Ziel ist es, die Privatsphäre der Bürger zu schützen und ihnen mehr Kontrolle über ihre Daten zu geben.

Im Facility Management spielt die DSGVO eine wichtige Rolle, da hier oft personenbezogene Daten von Mietern, Kunden, Mitarbeitern oder Dienstleistern verarbeitet werden. Dazu gehören Informationen wie Kontaktdaten, Zutrittskontrollen oder Videoüberwachung. Unternehmen im Facility Management müssen sicherstellen, dass sie diese Daten rechtmäßig und sicher verarbeiten, um den Anforderungen der DSGVO zu entsprechen. Dazu gehört auch die nachvollziehbare Information der Betroffenen über die Datennutzung und die Einhaltung von Löschfristen.

Der Zweck der DSGVO ist es, den Schutz der Privatsphäre und der personenbezogenen Daten zu gewährleisten und gleichzeitig den freien Datenverkehr innerhalb der EU zu ermöglichen. Unternehmen müssen geeignete Maßnahmen ergreifen, um die Sicherheit der Daten zu garantieren und sicherzustellen, dass nur die notwendigen Daten verarbeitet werden. Im Kontext des Facility Managements bedeutet dies, dass Prozesse zur Datenerfassung und -verarbeitung transparent, sicher und datensparsam gestaltet werden müssen, um den gesetzlichen Anforderungen zu entsprechen.[11]

EU Cyber Security Act
Der EU Cyber Security Act ist eine Verordnung der Europäischen Union, die einheitliche Standards für die Cybersicherheit von Produkten, Dienstleistungen und Prozessen in der EU schafft. Er stärkt die Rolle der Europäischen Agentur für Cybersicherheit (ENISA) und führt ein freiwilliges Zertifizierungssystem für IT-Produkte und -Dienste ein, um deren Sicherheitsniveau zu bewerten. Der EU Cyber Security Act soll das Vertrauen in digitale Technologien stärken und die Cybersicherheit in der gesamten EU verbessern.

Im Facility Management betrifft der EU Cyber Security Act insbesondere IT-Systeme und vernetzte Technologien, die zur Verwaltung von Gebäuden, Anlagen und Infrastruktur eingesetzt werden. Dazu gehören beispielsweise Smart-Building-Systeme, Zutrittskontrollen oder IoT-Geräte. Facility-Management-Unternehmen, die solche Systeme einsetzen, sollten darauf achten, dass diese Technologien nach anerkannten Sicherheitsstandards zertifiziert sind. Dies ist besonders wichtig, um Sicherheitslücken zu vermeiden, die unbefugten Zugriff auf sensible Daten oder Steuerungssysteme ermöglichen könnten.

[11] „Datenschutz-Grundverordnung (DSGVO)“, 2016 [Online]. Available: https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html

3.5.2 Normen

ISO/IEC 27001

Die ISO/IEC 27001 ist eine international anerkannte Norm, die Anforderungen an Informationssicherheit, Cybersicherheit und Datenschutz definiert. Sie beschreibt, wie ein Informationssicherheits-Managementsystem (ISMS) entwickelt, implementiert, aufrechterhalten und kontinuierlich verbessert werden kann. Dabei berücksichtigt sie den spezifischen Kontext der jeweiligen Organisation. Die ISO/IEC 27001 verfolgt das Ziel, geeignete Sicherheitsmaßnahmen für den Schutz sämtlicher Werte (Assets) innerhalb der Wertschöpfungsketten einer Organisation sicherzustellen. Dies gilt für Unternehmen jeder Art, einschließlich Handelsunternehmen, staatlicher Institutionen und Non-Profit-Organisationen. Der Schwerpunkt liegt dabei auf dem Schutz und der Sicherheit von Informationen und Daten. Durch die Einhaltung der ISO/IEC 27001 können Organisationen ihre Informationssicherheit effektiv stärken, Cyberangriffe abwehren und eine Zertifizierung nach internationalem Standard erreichen.[12]

IEC 62443-1+2

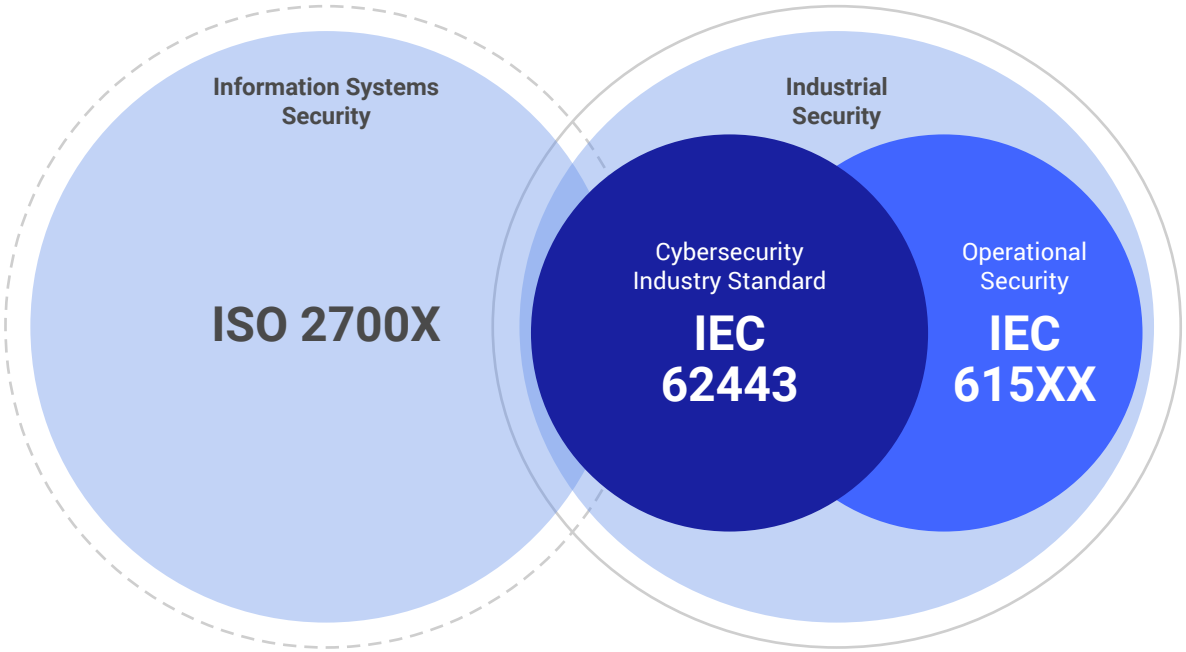
Die Normenreihe IEC 62443 ist ein international anerkannter Standard für die Cybersicherheit in der Automatisierungs- und Steuerungstechnik. Die Teile 1 und 2 dieser Norm befassen sich mit grundlegenden Konzepten, definierten Anforderungen und organisatorischen Maßnahmen zur Verbesserung der Sicherheit industrieller Automatisierungssysteme. Ziel ist es, die Informations- und Betriebssicherheit solcher Systeme über ihren gesamten Lebenszyklus hinweg zu gewährleisten. Dies umfasst den Schutz vor unbefugtem Zugriff, den Schutz sensibler Daten sowie die Sicherstellung der Systemverfügbarkeit.
Die Norm IEC 62443-1 legt die Grundlagen und Begriffe für die Cybersicherheit fest. Sie definiert allgemeine Sicherheitskonzepte, beschreibt Bedrohungsszenarien und stellt ein Rahmenwerk für die Entwicklung sicherer Systeme bereit. Die Norm ist relevant für alle, die industrielle Systeme planen, betreiben oder instandhalten, einschließlich der Bereiche Gebäudemanagement, Facility Management und Immobilienverwaltung.
IEC 62443-2 konzentriert sich auf organisatorische Maßnahmen und Anforderungen. Sie definiert Prozesse und Vorgehensweisen, die Unternehmen implementieren müssen, um ein wirksames Cybersicherheitsmanagementsystem zu etablieren. Dies umfasst die Identifikation von Risiken, die Durchführung von Sicherheitsbewertungen sowie die Festlegung von Richtlinien und Prozessen für den sicheren Betrieb.
Für Unternehmen im Gebäudemanagement, Facility Management und in der Immobilienverwaltung ist die Einhaltung dieser Normen besonders wichtig, da moderne Gebäude zunehmend vernetzt und automatisiert sind. Systeme wie Gebäudeleittechnik, Zugangskontrollsysteme und energieeffiziente Steuerungen sind auf verlässliche Cybersicherheit angewiesen, um den Betrieb sicher und störungsfrei zu gewährleisten. Durch die Anwendung der IEC 62443 können Unternehmen Sicherheitsrisiken gezielt minimieren und ihre technischen Infrastrukturen besser gegen potenzielle Bedrohungen absichern.[13]

[12] „ISO/IEC 27001“, 15.01.2025 [Online]. Available: https://cyberzoni.com/standards/iso-27001

[13] „IEC 62443“, 15.01.2025 [Online]. Available: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

Im Kontext der Cybersicherheit ist es wichtig, zwischen den Begriffen “Safety” und “Security” zu unterscheiden. Während “Safety” die Betriebssicherheit bezeichnet und den Schutz des Menschen und der Umwelt vor Maschinen zum Ziel hat, bezieht sich “Security” auf den Schutz der Daten von Maschinen und zielt darauf ab, ungewollte oder nicht autorisierte Veränderungen zu verhindern. Diese Veränderungen können nicht nur durch einen “Hacker” verursacht werden, sondern auch durch ungewollte oder nicht befugte Handlungen.

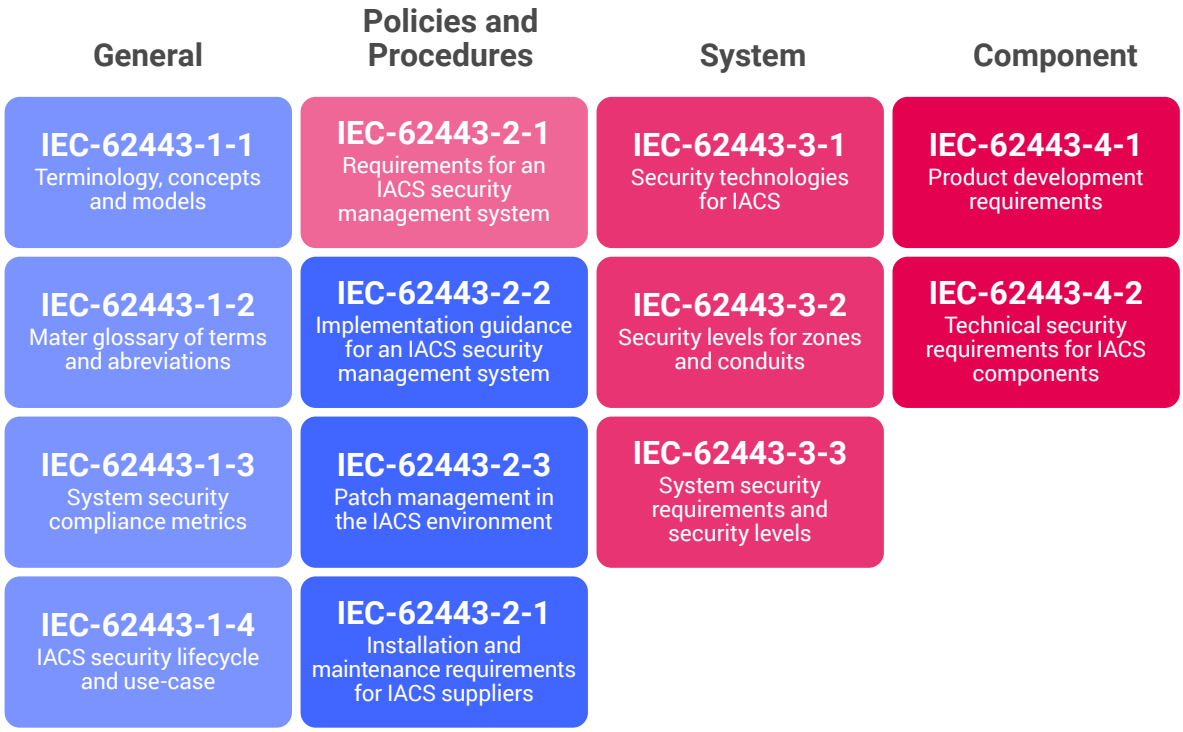
Abbildung 4: Übersicht über ISO 2700x und IEC[1]



Die IEC62443 bietet hierbei eine gute Grundlage zur Vermittlung beider Aspekte aus OT (Safety) und IT(Security). Die Implementierung des Standards erfordert hierbei eine einheitliche Betrachtung aller angedachten Maßnahmen zum Schutz von Leben und Werten aus beiden Welten.

[1] Kevin Wennemuth, CID GmbH, 2024

Abbildung 5: Detaillierte Übersicht über die IEC[1]



TRBS 1115 Teil 1

Die Technische Regel für Betriebssicherheit TRBS 1115 Teil 1 befasst sich mit den Maßnahmen zur Cybersicherheit sicherheitsrelevanter Mess-, Steuer- und Regelungseinrichtungen (MSR) in Arbeitsmitteln sowie überwachungsbedürftigen Anlagen. Diese Einrichtungen müssen nach dem Stand der Technik vor Cyberbedrohungen geschützt werden, um Gefährdungen für Beschäftigte und andere Personen im Gefahrenbereich zu vermeiden. Die Regel definiert zudem Anforderungen und Verantwortlichkeiten zur Sicherstellung der Cybersicherheit in diesen kritischen Systemen. Zu den betroffenen Bereichen gehören vor allem industrielle Anlagen, kritische Infrastrukturen und Arbeitsmittel, die eine Verbindung zu Netzwerken aufweisen und somit potenziell anfällig für Cyberangriffe sind.[14 & 15]

[14] „GMBI, Nr. 25“, 11.2022 [Online]. Available: https://baua.de

[15] „TRBS 1115, Teil 1“, 15.01.2025 [Online]. Available: https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1

3.5.3 Richtlinien

BSI-Grundschutzkataloge
Die BSI-Grundschutzkataloge sind eine Sammlung von Richtlinien, Maßnahmen und Empfehlungen, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bereitgestellt werden, um Unternehmen und Behörden dabei zu unterstützen, ihre IT-Sicherheit auf ein hohes Niveau zu bringen. Die Kataloge bieten einen systematischen Ansatz, um Risiken zu identifizieren und durch standardisierte Maßnahmen zu minimieren. Sie richten sich an Organisationen jeder Größe und Branche.

Im Facility Management sind die BSI-Grundschutzkataloge besonders wichtig, wenn es um die Absicherung von IT-Systemen geht, die zur Steuerung und Verwaltung von Gebäuden, Anlagen und kritischen Infrastrukturen verwendet werden. Facility-Management-Systeme, wie etwa Gebäudeautomationssysteme, Zutrittskontroll- oder Überwachungssoftware, sind häufig mit Netzwerken verbunden und somit potenziellen Cyberangriffen ausgesetzt. Der BSI-Grundschutz hilft dabei, diese Systeme abzusichern, um den Betrieb und die Sicherheit der verwalteten Infrastrukturen zu gewährleisten.

Im Facility Management sind besonders folgende Bereiche der BSI-Grundschutzkataloge relevant:

- INF.13 – Technisches Gebäudemanagement (TGM): Richtlinie für Planung, Umsetzung und Betrieb der Technischen Gebäudeausrüstung
- INF.14 – Gebäudeautomation: Informationssicherheit in Planung, Realisierung und Betrieb von Gebäudeautomation
- INF.2 – Rechenzentrum: Sicherheitsvorgaben für IT-Infrastrukturen in Rechenzentren, die oft mit Facility-Management-Systemen verknüpft sind
- APP.3 – Webanwendungen: Schutz von webbasierten Facility-Management-Plattformen
- OPS.1 – Serverbetrieb: Absicherung der Server, auf denen Facility-Management-Software läuft
- CON.5 – Notfallmanagement: Maßnahmen zur Sicherstellung des Betriebs und Wiederherstellung von Gebäudemanagementsystemen im Krisenfall.

Durch die Anwendung dieser Bausteine lassen sich Sicherheitsrisiken für IT-Systeme im Facility Management reduzieren und ein reibungsloser Betrieb gewährleisten.

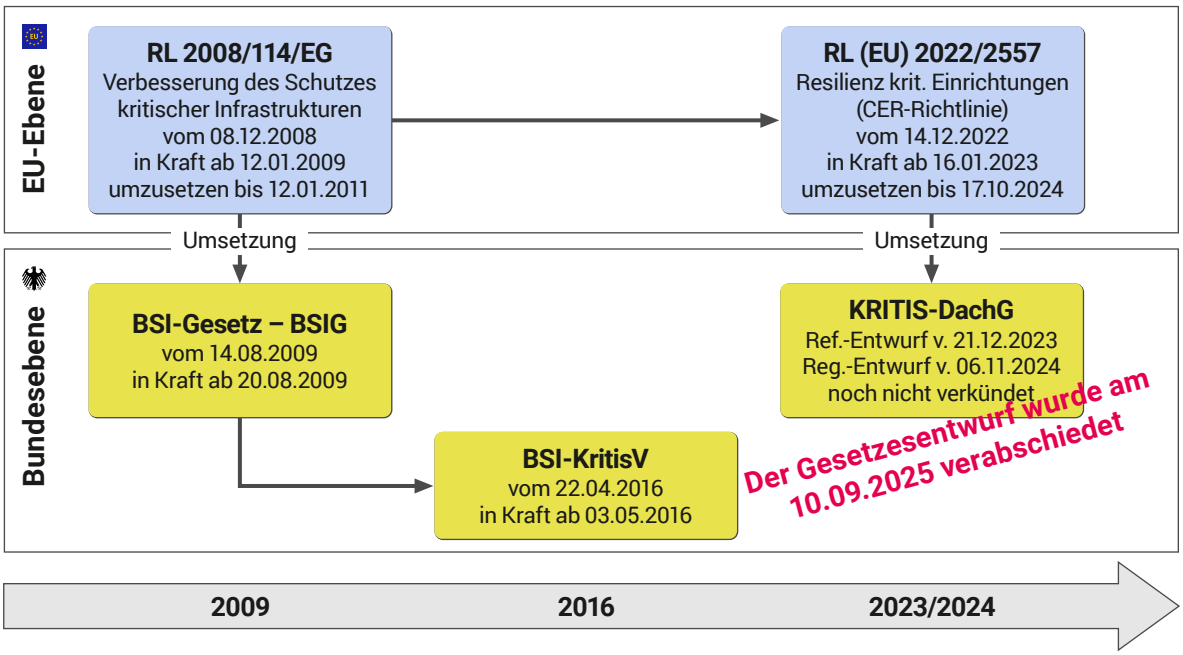
Der Baustein BSI INF.13 beschreibt, wie die IT-Sicherheit in Gebäudemanagementsystemen umgesetzt werden kann. Der Baustein befasst sich insbesondere mit der Verwaltung von Gebäuden und technischen Anlagen und gibt konkrete Empfehlungen zur sicheren Integration und Verwaltung von IT-Komponenten in Gebäudeautomationssystemen. Zu den zentralen Themen gehören der Schutz von Steuerungssystemen, die Zugriffskontrolle, Datensicherung und sichere Anbindung an Netzwerke. INF.13 hilft dabei, IT-Risiken im Gebäudemanagement zu reduzieren und den sicheren Betrieb von Gebäuden und technischen Anlagen zu gewährleisten.[8]

[8] „BSI-Grundschutzkataloge“, 15 01 2025. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.htm

KRITIS-Verordnung (BSI-KritisV)

Die KRITIS-Verordnung (Verordnung über Kritische Infrastrukturen) definiert in Deutschland, welche Unternehmen und Einrichtungen zu den sogenannten kritischen Infrastrukturen (KRITIS) zählen. Diese betreffen lebenswichtige Bereiche wie Energie, Wasser, Ernährung, Gesundheit, Transport und Informationstechnik.
Grundlage der KritisV ist die europäische Richtlinie 20008/114/EG (Verbesserung zum Schutz kritischer Infrastrukturen) aus dem Jahr 2009, die in Deutschland mit dem BSI-Gesetz vom August 2009 umgesetzt wurde. Erweiterte Anforderungen an die Resilienz kritischer Einrichtungen wurden in der europäischen Richtlinie 2022/2557 formuliert. Die Richtlinie wird in Deutschland durch das KRITIS DachG umgesetzt. Der Gesetzesentwurf wurde am 10.09.2025 verabschiedet.

Abbildung 6: KRITIS-Verordnung (BSI-KritisV)



Unternehmen, die unter die Verordnung fallen, müssen Maßnahmen ergreifen, um die Sicherheit und Funktionsfähigkeit ihrer Technologien und Infrastruktur vor Cyberangriffen zu schützen, um die Versorgungssicherheit zu gewährleisten.[16] Sie werden verpflichtet regelmäßige Risikoanalysen durchzuführen und einen Resilienzplan zu erstellen.

Im Facility Management ist die KRITIS-Verordnung relevant, wenn Unternehmen oder öffentliche Einrichtungen Anlagen betreiben, die zu kritischen Infrastrukturen gehören, wie etwa in Krankenhäusern, Wasserversorgungsunternehmen oder bei Energieversorgern. Für diese Einrichtungen müssen spezielle

[16] „KRITIS-Verordnung (BSI-KritisV)“, 15.01.2025 [Online]. Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KM4/KRITIS-Dachgesetz.html

Sicherheitsanforderungen eingehalten werden, um den Betrieb und die Verfügbarkeit der Infrastruktur sicherzustellen. Facility-Management-Dienstleister müssen daher sicherstellen, dass die eingesetzten technischen Systeme, wie z. B. Gebäudeverwaltungs-, Sicherheits- und Überwachungssysteme, erhöhten Sicherheitsanforderungen genügen.

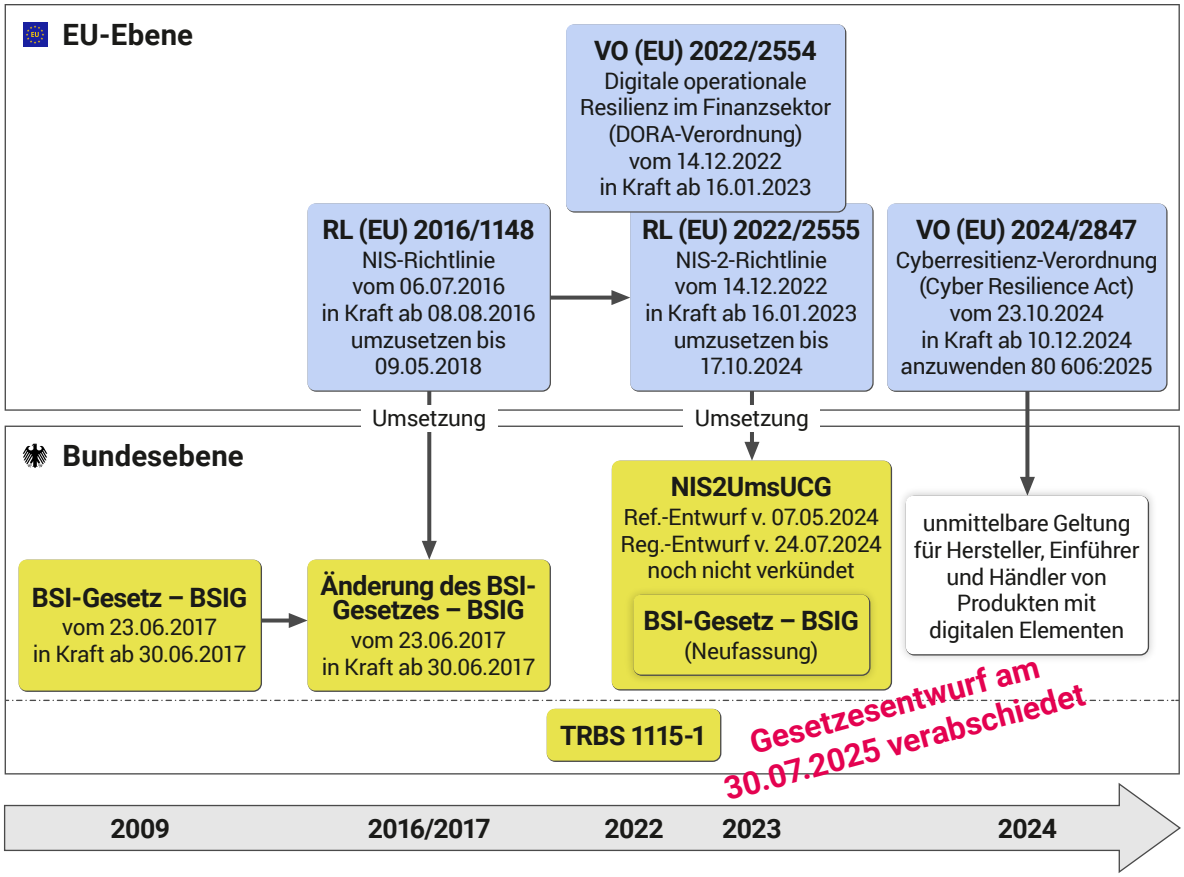
EU-NIS-Richtlinie/NIS-2-Richtlinie

Die EU-NIS-Richtlinie (Richtlinie über die Sicherheit von Netz- und Informationssystemen) wurde eingeführt, um die Cybersicherheit in der EU zu verbessern. Sie verpflichtet Betreiber wesentlicher Dienste, darunter Energie, Verkehr, Wasser und Gesundheit, sowie digitaler Dienste, Maßnahmen zur IT-Sicherheit zu ergreifen und Vorfälle zu melden. Die Richtlinie soll sicherstellen, dass kritische Infrastrukturen vor Cyberbedrohungen geschützt und ihre Betriebsfähigkeit gesichert sind.

Im Facility Management ist die NIS-Richtlinie relevant, wenn Unternehmen kritische Infrastrukturen betreuen, wie z. B. Wasserversorgung, Gesundheitsdienste oder Energieversorgung. Systeme, die diese Infrastrukturen steuern, wie Gebäudemanagement und Überwachungssysteme, müssen den Anforderungen der NIS-Richtlinie entsprechen.

Die NIS-2-Richtlinie, die die ursprüngliche NIS-Richtlinie aktualisiert, erweitert den Anwendungsbereich auf mehr Sektoren, wie Postdienste, Abfallwirtschaft und öffentliche Verwaltung, und verschärft die Sicher-

Abbildung 7: EU-NIS-Richtlinie/NIS-2-Richtlinie



heitsanforderungen. Sie sieht strengere Meldepflichten für Sicherheitsvorfälle und höhere Sanktionen bei Nichteinhaltung vor.
Der EU Cyber Security Act ergänzt NIS-2, indem er ein europaweites Zertifizierungssystem für IT-Produkte und -Dienste schafft. Diese Zertifizierungen stellen sicher, dass IT-Lösungen, die in kritischen Infrastrukturen und von wesentlichen Diensten verwendet werden, nach anerkannten Sicherheitsstandards geprüft sind. Im FM-Kontext stellt dies sicher, dass die eingesetzten Technologien zur Gebäudeverwaltung und Anlagensteuerung sowohl den Vorgaben von NIS-2 als auch den höchsten Sicherheitsstandards gemäß Cyber Security Act entsprechen.
Die Umsetzung der europäischen NIS2 Richtlinie in deutsches Recht wird mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) verfolgt. Der Gesetzesentwurf wurde am 30.7.2025 verabschiedet..[17 & 23]

3.5.4 Zertifikate

Im Facility Management sind Zertifizierungen mit Bezug zur Cybersicherheit besonders wichtig, da moderne Gebäude- und Anlagenmanagementsysteme immer stärker vernetzt und digitalisiert sind. Viele dieser Systeme steuern kritische Infrastrukturen wie Energie, Wasser oder Zugangskontrollen.

Durch die Einhaltung von Cybersicherheit-Zertifizierungen wird sichergestellt, dass:

- Sensible Daten wie Gebäudezugänge oder Betriebsdaten sicher verwaltet werden
- Kritische Systeme vor Cyberangriffen geschützt sind, die den Betrieb von Gebäuden oder Infrastrukturen stören könnten
- Compliance mit gesetzlichen Anforderungen, wie der DSGVO oder KRITIS-Vorgaben, gewährleistet ist

Zertifizierungen wie ISO 27001, BSI IT-Grundschutz oder die EU Cyber Security Act-Zertifikate bieten eine strukturierte Grundlage, um die IT-Sicherheit zu erhöhen, rechtliche Anforderungen zu erfüllen und das Vertrauen von Kunden und Partnern im Facility Management zu stärken. Im Folgenden sind einige dieser Zertifizierungen kurz erklärt.

Zertifizierung nach ISO/IEC 27001
Die internationale Norm ISO/IEC 27001 legt Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) fest. Eine ISO 27001-Zertifizierung hilft Facility-Management-Unternehmen dabei, ihre IT-Systeme strukturiert zu schützen, indem sie Risiken analysiert und Sicherheitsmaßnahmen benennt. Sie ist besonders relevant für den Schutz von Daten, die in IT-gestützten Gebäudemanagementsystemen verarbeitet werden.[12]

[17] „NIS-Richtlinie“, 15.01.2025 [Online]. Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html
[23] „EU-Rechtsakt zur Cyberresilienz“, 15.01.2025 [Online]. Available: https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act
[12] „ISO/IEC 27001“, 15.01.2025 [Online]. Available: https://cyberzoni.com/standards/iso-27001

Zertifizierung als KRITIS-Unternehmen gemäß § 8a BSIG
Die Zertifizierung für Betreiber kritischer Infrastrukturen (KRITIS) gemäß § 8a Bundesamt für Sicherheit in der Informationstechnik Gesetz (BSIG) ist eine wichtige rechtliche Anforderung für Unternehmen, die kritische Infrastrukturen betreiben. Diese Vorschrift verpflichtet Betreiber von Einrichtungen, die für das Funktionieren des Gemeinwesens von wesentlicher Bedeutung sind, zu besonderen Sicherheitsvorkehrungen, um ihre IT-Systeme und Netzwerke vor Cyberangriffen zu schützen und sicherzustellen, dass sie auch bei Störungen funktionsfähig bleiben.

Im Facility Management ist die KRITIS-Zertifizierung von besonderer Relevanz, wenn Unternehmen Gebäude oder Anlagen verwalten, die als kritische Infrastrukturen eingestuft sind, wie Energieversorgungseinrichtungen, Wasserwerke oder Gesundheitseinrichtungen. Facility-Management-Dienstleister müssen sicherstellen, dass ihre Systeme zur Gebäudeverwaltung, wie z. B. Heizungs-, Lüftungs- und Klimaanlagen (HVAC) sowie Sicherheits- und Überwachungssysteme, den Anforderungen des § 8a BSIG entsprechen.

Die KRITIS-Zertifizierung erfordert von diesen Unternehmen, dass sie umfassende Sicherheitsmaßnahmen implementieren, um die Integrität und Verfügbarkeit ihrer IT-Systeme zu gewährleisten. Dies umfasst unter anderem die Durchführung regelmäßiger Risikoanalysen, die Implementierung von Sicherheitsvorkehrungen sowie Notfall- und Wiederherstellungsplänen. Die Einhaltung dieser Vorgaben stellt sicher, dass die kritischen Infrastrukturen, die durch Facility-Management-Systeme unterstützt werden, auch im Falle eines Cyberangriffs oder technischen Ausfalls zuverlässig betrieben werden können.[9]

C5-Zertifizierung (Cloud Computing Compliance Criteria Catalogue)
Die C5-Zertifizierung (Cloud Computing Compliance Criteria Catalogue) ist ein Sicherheitsstandard, der speziell für Cloud-Dienste entwickelt wurde. Sie wurde vom BSI in Deutschland erstellt und bietet eine umfassende Grundlage für die Bewertung und Zertifizierung der Sicherheitsmaßnahmen von Cloud-Anbietern.

Zweck der C5-Zertifizierung ist es, Cloud-Dienstleistern und deren Kunden eine transparente und verlässliche Möglichkeit zu bieten, die Sicherheitsmaßnahmen und Compliance-Anforderungen von Cloud-Services zu überprüfen. Die Zertifizierung basiert auf einem Katalog von Sicherheitsanforderungen, die von Cloud-Anbietern erfüllt werden müssen, um die Vertraulichkeit, Integrität und Verfügbarkeit der bereitgestellten Cloud-Dienste zu gewährleisten.

Wichtige Aspekte der C5-Zertifizierung sind

- Sicherheitsmanagement: Die C5-Zertifizierung prüft, ob Cloud-Anbieter ein umfassendes Sicherheitsmanagementsystem implementiert haben, das alle relevanten Sicherheitsrisiken abdeckt.
- Datenschutz: Die Zertifizierung stellt sicher, dass Cloud-Anbieter Datenschutzanforderungen erfüllen, insbesondere im Hinblick auf die sichere Verarbeitung und Speicherung von personenbezogenen Daten.
- Compliance: C5 fordert die Einhaltung von gesetzlichen und regulatorischen Anforderungen, die für Cloud-Dienste relevant sind.

[9] „BSIG-, BSI-, IT-Sicherheitsgesetz“, 15.01.2025 [Online]. Available: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html; C5-Zertifizierung (Cloud Computing Compliance Criteria Catalogue)

Im FM ist die C5-Zertifizierung von Bedeutung, wenn Cloud-basierte Systeme und Dienste zur Verwaltung von Gebäuden, Anlagen oder technischen Einrichtungen genutzt werden. Die C5-Zertifizierung stellt sicher, dass die Cloud-Dienste, die für das Gebäudemanagement verwendet werden, sicher und zuverlässig sind, insbesondere im Hinblick auf Datenschutz und Datensicherheit. Dies ist besonders wichtig für die Sicherheit von sensiblen Betriebsdaten und Systemen, die für die effiziente und sichere Verwaltung von Gebäuden und technischen Infrastrukturen verantwortlich sind. Durch die C5-Zertifizierung können Facility-Management-Unternehmen sicherstellen, dass ihre Cloud-Dienste den höchsten Sicherheitsstandards entsprechen und den gesetzlichen Anforderungen entsprechen.[18]

Zertifizierung nach IEC 62443

Die Zertifizierung nach IEC 62443 bestätigt, dass Unternehmen, Produkte oder Systeme die definierten Sicherheitsanforderungen der Norm erfüllen. Der Zertifizierungsprozess umfasst Prüfungen, Audits und Sicherheitsbewertungen durch unabhängige Stellen. Dies bietet Unternehmen einen glaubwürdigen Nachweis ihrer Sicherheitskompetenz und stärkt das Vertrauen von Kunden und Partnern.
Für Unternehmen im Gebäudemanagement, Facility Management und in der Immobilienverwaltung ist die Einhaltung und Zertifizierung nach IEC 62443 von wachsender Bedeutung. Moderne Gebäude sind durch vernetzte Systeme wie Gebäudeleittechnik, Zugangskontrollsysteme und energieeffiziente Steuerungen zunehmend cyber-physisch vernetzt. Die Zertifizierung stellt sicher, dass diese Systeme gegen potenzielle Cyberbedrohungen abgesichert sind und der sichere Betrieb der technischen Infrastruktur gewährleistet ist. Unternehmen profitieren durch eine höhere Betriebssicherheit, reduzierte Ausfallrisiken und gesteigertes Vertrauen in ihre digitalen Systeme.[13]

Zertifizierung durch und auf Basis des BSI

Die Zertifizierung durch das BSI oder auf dessen Basis bietet einen verlässlichen Rahmen für Cybersicherheit in Deutschland. Das BSI zertifiziert IT-Produkte, -Dienstleistungen und -Systeme nach strengen Sicherheitsanforderungen. Dazu gehören Sicherheitszertifikate für Hardware, Software und Netzwerksysteme, die durch unabhängige Prüfungen und Audits bestätigt werden.
Für das Facility Management und das Gebäudemanagement gewinnt diese Zertifizierung zunehmend an Bedeutung. Moderne Gebäude sind durch intelligente Systeme wie Gebäudeleittechnik, Zugangskontrollsysteme und smarte Energiemanagementlösungen digital vernetzt. Diese Systeme sind potenziellen Cyberbedrohungen ausgesetzt und erfordern umfassende Sicherheitsmaßnahmen.
BSI-zertifizierte Lösungen bieten hier einen entscheidenden Vorteil: Sie gewährleisten, dass technische Systeme und IT-Komponenten nach anerkannten Sicherheitsstandards entwickelt und betrieben werden. Facility Manager können durch den Einsatz zertifizierter Produkte und Dienstleistungen die Betriebssicherheit erhöhen, Ausfallrisiken minimieren und die Einhaltung gesetzlicher und regulatorischer Anforderungen sicherstellen. Dies schafft Vertrauen bei Eigentümern, Mietern und Investoren und unterstützt eine nachhaltige und sichere Bewirtschaftung von Immobilien.[19]

[18] „BSI – Cloud Security“, 15.01.2025 [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_AktuelleVersion/C5_AktuelleVersion_node.html

[13] „IEC 62443“, 15.01.2025 [Online]. Available: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

[19] „Zertifizierung BSI“, 15.01.2025 [Online]. Available: www.bsi.bund.de/zertifizierung

4 Mögliche Einfallstore, Anwendungen und Risiken

Alle netzwerkfähigen Geräte können als Einfallstore für Cyberattacken dienen. Entscheidend ist, wie die Geräte konfiguriert sind. Werden Standardpasswörter nicht ersetzt, offene physische Schnittstellen bereitgestellt oder unverschlüsselte Kommunikationsprotokolle verwendet, so wird einem möglichen Angriff nichts entgegengesetzt.
Weiterhin ist die Anbindung an das IT-Netz für die Reichweite des Angriffes entscheidend. Ist die Komponente in ihrem Subnetz nicht isoliert, so kann ein Zugriff weit in die Unternehmens-IT ermöglicht werden.

4.1 Cyberangriffe auf Aufzüge

Die Risiken von Cyberangriffen auf Aufzüge sind real und die Notwendigkeit, Schutzmaßnahmen nachzuweisen, ist nun gesetzlich vorgeschrieben. Betreiber von Aufzugsanlagen sind nun verpflichtet, im Rahmen ihrer Gefährdungsbeurteilung mögliche Cyberbedrohungen zu identifizieren, geeignete Schutzmaßnahmen zu treffen und diese angemessen zu dokumentieren.
Digitalisierte und vernetzte Aufzüge bieten viele Vorteile, sind jedoch auch anfällig für Angriffe. Dies betrifft nicht nur neue, sondern auch ältere Aufzüge, zum Beispiel aufgrund eines vorhandenen Notrufsystems oder der Modernisierung von Komponenten, die durch Nachrüstungen oder Notrufsysteme vernetzt sind. Wenn Software oder Schnittstellen nicht ausreichend geschützt sind, können Funktionen manipuliert werden.
Mit der fortschreitenden Digitalisierung werden Anlagen wie Aufzüge immer digitaler und vernetzter. Gesetze und Verordnungen folgen jedoch nicht unmittelbar der Einführung neuer Technologien, sondern treten erst nach der jeweiligen technischen Entwicklung in Kraft.
Im März 2023 hat der Gesetzgeber die neue Technische Regel für Betriebssicherheit[15] verabschiedet. Die Technische Regel für Betriebssicherheit TRBS 1115-1 konkretisiert hier die Betriebssicherheitsverordnung bezüglich der Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen („MSR-Einrichtungen“) sowie weitere schutzbedürftige Komponenten (z. B. Notrufsystem). Auf Grundlage dieser TRBS können Betreiber mögliche Cybergefährdungen identifizieren, geeignete Schutzmaßnahmen treffen sowie ihre Gefährdungsbeurteilung entsprechend aktualisieren. Legen sie bei der wiederkehrenden Prüfung (Hauptprüfung), Prüfung vor Inbetriebnahme und vor Wiederinbetriebnahme nach prüfpflichtigen Änderungen keine anlagenspezifische Dokumentation vor, erscheint dies als Mangel in der Prüfbescheinigung. TRBS sind Konkretisierungen der Betriebssicherheitsverordnung und gelten unter anderem für den Betrieb von Aufzugsanlagen.
Betreiber sind verantwortlich für die Analyse möglicher Gefährdungen durch Cyberbedrohungen und die Umsetzung geeigneter Gegenmaßnahmen. Die bestehende Gefährdungsbeurteilung sollte um die Betrachtung von Cyberbedrohungen erweitert werden. Die TRBS 1115 Teil 1 (gilt fortlaufend) bietet eine Hilfestellung dafür, wie dies aussehen kann.

[15] „TRBS 1115, Teil 1“, 15.01.2025 [Online]. Available: https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1

Die rechtlichen Grundlagen sind das Gesetz über überwachungsbedürftige Anlagen (ÜAnlG), die Betriebssicherheitsverordnung (BetrSichV) und zur Konkretisierung die Technische Regel für Betriebssicherheit TRBS 1115-1.
Nach BetrSichV / ÜAnlG hat der Betreiber die Pflicht, im Rahmen seiner Gefährdungsbeurteilung alle relevanten Komponenten aufzulisten und sie hinsichtlich möglicher Gefährdungen durch Cyberbedrohungen zu bewerten. Die TRBS 1115-1 gibt vor, wie Cybersicherheitsmaßnahmen zu ermitteln sind und welche Maßnahmen festzulegen sind.
„Sicherheitsrelevante MSR-Einrichtungen dienen der Verhinderung von Gefährdungen bei der Verwendung von Arbeitsmitteln, die nicht durch inhärent sichere Konstruktion des Arbeitsmittels oder durch trennende Schutzeinrichtungen beseitigt oder ausreichend vermindert werden können“ (Definition TRBS 1115). Im Kontext von Aufzügen sind sicherheitsrelevante MSR-Einrichtungen vorhanden, wenn die Sicherheit mit Hilfe von programmierbarer Elektronik gewährleistet wird, anstelle von konventioneller Elektrik und Mechanik.
Ob an einer Anlage sicherheitsrelevante MSR-Einrichtungen verbaut sind, kann nicht pauschal beantwortet werden. Informationen dazu finden sich in der Anlagendokumentation oder in einer zentralen Plattform für die digitale Organisation der Anlagenprüfung wie z. B. in netinform des TÜV SÜD.
Es ist wichtig zu beachten, dass Betreiber in der Gefährdungsbeurteilung stets alle Gefährdungen bewerten müssen. Die TRBS 1115 Teil 1 ist eine Vorgabe wie Cyberbedrohungen an sicherheitsrelevanten MSR-Einrichtungen zu behandeln sind. Man kann das Vorgehen aber analog für weitere schutzbedürftige Komponenten (z. B. ein Notrufsystem) nutzen – um alle potenziellen Gefährdungen durch Cyberbedrohungen zu bewerten bzw. einzubeziehen.
Bei der Prüfung muss dem Sachverständigen nachgewiesen werden, dass Gefährdungen durch Cyberbedrohungen an der Anlage bewertet wurden. Liegt kein Nachweis vor, so wird dies in der Prüfbescheinigung beanstandet. Der Sachverständige führt anschließend eine Plausibilitätsprüfung des Nachweises durch. Die Plausibilitätsprüfung ist eine Ordnungsprüfung, bei der die Dokumentation des Betreibers bzgl. Cybersicherheit auf Vollständigkeit, Plausibilität und Nachvollziehbarkeit geprüft wird. Die Prüfung der Funktionsfähigkeit der festgelegten Maßnahmen ist nicht Bestandteil einer Ordnungsprüfung und erfolgt zu einem späteren Zeitpunkt. Den Betreiber entbindet es aber nicht davon, die Vorgaben der TRBS 1115 Teil 1 vollumfänglich umzusetzen.

Die Betriebssicherheitsverordnung (BetrSichV) richtet sich zwar an Arbeitgeber, aber das Gesetz über überwachungsbedürftige Anlagen (ÜAnlG) regelt in §4, dass jeder Betreiber einer überwachungsbedürftigen Anlage eine Gefährdungsbeurteilung erstellen muss und dass die Gefährdungen, die beim Betrieb von derartigen Anlagen auftreten können, zu beurteilen sind.

Dies betrifft u. a. Aufzugsanlagen die gewerblichen oder wirtschaftlichen Zwecken dienen oder durch die Beschäftige gefährdet werden können [vgl. ÜAnlG §2]. Wenn z. B. eine Hausverwaltung einen Hausmeister beschäftigt oder Vermieter die Kosten des Aufzugs über die Nebenkosten an die Mieter weitergeben, liegt das Dienen eines wirtschaftlichen Zwecks des Aufzugs vor. Nur Aufzüge, die wirklich keinem wirtschaftlichen Zweck dienen, bilden die Ausnahme.

Die Frage der Cybersicherheit ist nicht ausschließlich ein Thema, das vom Anlagenhersteller geregelt werden muss. Technische Regeln für Betriebssicherheit behandeln den Betrieb von Anlagen und richten sich daher an die Betreiber.
Es ist wichtig zu beachten, dass es bereits seit Mitte 2022 eine ISO-Norm zur Cybersicherheit an Aufzugsanlagen gibt, die ISO 8102-20. Diese Norm ist jedoch nicht harmonisiert und stellt daher keine Verpflichtung für Hersteller dar. Sie behandelt nicht nur sicherheitsrelevante MSR-Einrichtungen, sondern auch Security-Maßnahmen für alle Anlagenteile des Aufzugs, wie die Steuerung und das Notrufsystem.[20]

[20] „Cyberangriffe auf Aufzüge“, 15.01.2025 [Online]. Available: https://www.tuvsud.com/de-de/branchen/real-estate/technische-gebaeudeausruestung-und-aufzuege/aufzuege-fahrtreppen-foerdertechnik/aufzug-cybersicherheit

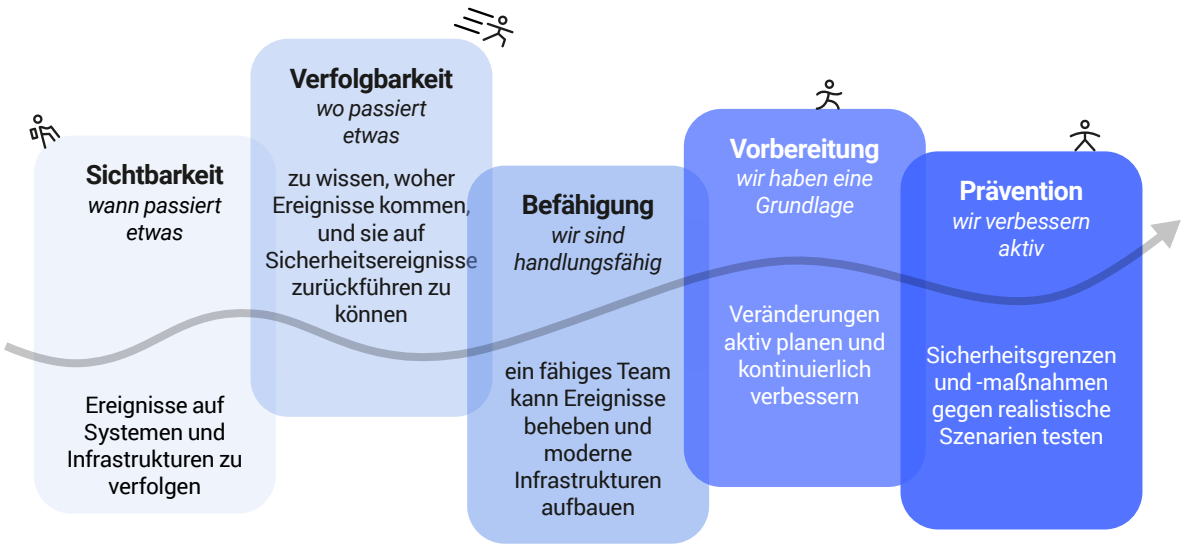
5 Wesentliche Maßnahmen

Maßnahmen zur Bildung und Optimierung von Cyberresilienz sind immer mit Augenmaß zu betrachten. Effektivität in der Verstärkung der eigenen Resilienz finden sich meist an ungewöhnlichen Orten. Laut einer Gartner Studie zum Thema TOP IT Security Vorhersagen von 2016 ist ein Drittel aller anfallenden Kosten in IT-Abteilungen auf Schatten-IT zurückzuführen. Eben jenes Drittel bildet hierbei auch das größte Risiko für Cyberangriffe jeglicher Art.

Warum ist das so gefährlich? Wie der Name schon sagt, befindet sich die Schatten-IT außerhalb der Erfassung (und damit auch des Schutzes) der regulären IT. Da benötigt der Kollege „mal eben schnell“ ein neues System, irgendwo lauert noch ein Altsystem herum oder der Azubi bringt seinen Router mit, weil die Internetfilterung so nervig ist. All diese Systeme unterliegen keinem methodischen Schutz und bilden Einfallstore für böswillige Akteure.

Eine der ersten Maßnahmen zur Erhöhung der Cyberresilienz ist damit die Schaffung von Transparenz der IT-Landschaft als Ganzes.

Abbildung 8: Wesentliche Maßnahmen[1]



Nachdem nun bekannt ist, wo sich evtl. gefährdete Systeme befinden, ist es daran, diese auch transparent in ihren Abläufen zu machen (Verfolgbarkeit). Zu wissen, „wo die Dinge passieren“ und in der Lage zu sein, Ereignisse von Anfang bis Ende zu verfolgen, ist entscheidend für die Implementierung der IT-Sicherheit.

[1] Kevin Wennemuth, CID GmbH, 2024

Doch was hilft all die Technik, wenn wir keine Menschen verfügbar haben, die mit den ermittelten Daten auch umgehen, reagieren und arbeiten können? Wie oft kommt es vor, dass eben jener Kollege im Urlaub ist, der das System als einziger kennt? Diesem Bus-Faktor muss gezielt begegnet werden. Geschulte und qualifizierte Mitarbeiter sollten in alle Prozesse, Abläufe und das Management einbezogen werden. Feedbackprozesse und kontinuierliche Verbesserungen können nur so etabliert werden.

Wie beim Fußball hilft es nicht, nur am Rand zu stehen, alle Regeln besser als der Schiedsrichter zu kennen und die Spieler „anzufeuern". Es ist notwendig, selbst auf das Spielfeld zu gehen und zu lernen, wie das Spiel unter realen und auch wechselnden Bedingungen funktioniert. Wir müssen proaktiv Schulungen, Bedrohungsanalysen, Penetrationstests und geplante Hackathons durchführen. Wir müssen uns gezielt und methodisch auf die Auswirkungen sicherheitsrelevanter Ereignisse durch gezieltes praktisches Training vorbereiten.

Fragen aus der IT, die man sich auch in FM gezielt im Kontext der OT-Sicherheit stellen kann:

- Alle unsere Passwörter sind gerade veröffentlicht worden! Was nun?
- Welche IT-Security Maßnahmen wurden bzgl. der Gebäudesoftware festgelegt?
- Wie lange reicht eigentlich unser Cashflow, wenn die gesamte IT stillsteht?
- Wie lange brauchen unsere Backups in der Wiederherstellung?
- Wen rufe ich im Cyber-Notfall an?
- Was mache ich, wenn ein Fremdzugriff ins GLT-Netz besteht?

Und nachdem wir geschwitzt und trainiert haben, sollten wir uns einer externen Prüfung unserer Fähigkeiten unterziehen. Wir wollen einen klaren Blick, ohne Beschönigung, auf unsere Sicherungsmaßnahmen. Die Weiterentwicklung aktueller Maßnahmen. Der Fokus liegt auf dem Identifizieren von Schwachstellen und diese zu reduzieren. Die Einrichtung von Feedbackzyklen zu all diesen Prozessen ist essenziell.

5.1 Technische Maßnahmen

Soll eine bestehende GLT erweitert oder umgebaut werden, oder wird eine neue Immobilie übernommen und soll in die bestehenden Strukturen integriert werden, so ist zunächst eine Bestandsanalyse der betriebenen GLT und Sicherheitstechnik notwendig.

In der Analyse müssen alle Subnetze, in denen Komponenten verbaut sind, und ihre Kommunikationsbeziehungen untereinander beschrieben werden. Kommunikations-Protokolle und verwendete Ports sowie die IP-Adressen der Komponenten sind ebenfalls zu benennen.

GLT-spezifische Protokolle (Bacnet[21]) und Netzwerktopologien werden aufgeführt und um die Produktfamilien und ggf. Versionsnummern ergänzt, um Handlungsoptionen für eine Optimierung ableiten zu können. Veraltete Hardware unterstützt teilweise keine verschlüsselte Kommunikation.
Alle in den Netzen lokalisierten Komponenten müssen benannt werden. Genauso sind alle mit diesen Komponenten interagierenden Server aus anderen Netzen z. B. GLT, Energie-Controlling-Systeme, Zentrale Leittechnik oder Monitoring-Systeme aufzuführen. Diese Netze und ihre weiteren Komponenten sind vollumfänglich zu beschreiben.
Insbesondere sind alle Verbindungswege in das Internet aufzuführen. Das BSI weist explizit darauf hin, „dass Bestandslösungen auf Basis von analogen oder ISDN-Modems sowie die direkte Internetanbindung von Komponenten wie Speicher-programmierbare Steuerungen (SPS) nicht dem aktuellen Stand der Technik genügen."

Die Netzwerkkomponenten der KNX- und Bacnet-Netze können in Form von Listen aufgestellt und bewertet werden. Bewertungsparameter sind der Stand der Firmware und des Herstellersupports, die Verschlüsselungs- und Authentifizierungsmethoden, der Überwachungsstatus und der Hinweis, ob bereits Anomalien erkannt wurden. Anhand des Ergebnisses kann eine Handlungsoption bestimmt werden.

Die Handlungsoptionen werden entsprechend der vorab festgelegten Sicherheitsanforderungen und -ziele bestimmt. Hierbei kann zwischen kurz-, mittel- und langfristigen Sicherheitszielen unterschieden werden. Kurzfristige Ziele können die sofortige Implementierung von Authentifizierungs- und Verschlüsselungsmechanismen und die Schulung des Personals in den neuen Sicherheitsprotokollen sein. Zu mittelfristigen Zielen kann die Einführung eines Überwachungs- und Alarmsystems und die Implementierung eines Lifecycle-Management-Systems für Hardware zählen. Langfristige Ziele wären die Entwicklung und Implementierung eines umfassenden Sicherheitsmanagementplans, die Investition in fortschrittliche Sicherheitslösungen und Technologien sowie die Etablierung einer Sicherheitskultur innerhalb der Organisation.

Im nächsten Schritt sind die Anforderungen an die Anbindung an zentrale IT-Dienste (z. B. Zeitserver, Mail-Relay) oder Monitoring Systeme aufzustellen.
Idealerweise wird ein Verfahren für die Bereitstellung von Wartungszugängen entwickelt. Das BSI empfiehlt Fernwartungszugriff möglichst nicht pauschal pro (Sub)Netz zu berechtigen, sondern vielmehr feingranu-

[21] „BACnet Committee", 07.02.2025 [Online]. Available: https://bacnet.org/

lar pro IP und Port zu regeln. Dies minimiert die „Reichweite von Fernwartungszugängen und beschränkt somit auch die Folgen einer Kompromittierung“. Fernwartungs-Clients sollten nur für diese Aufgabe betrieben werden.

Für die Konzeption von GLT-Netzen sind folgende Rahmenbedingungen einzuhalten:

- Die notwendige Internetkommunikation in die Subnetze erfolgt immer über eine Firewall auf einzeln freigegebene IP-Adressen.
- Innerhalb der Subnetze werden keine eigenen Internetverbindungen aufgebaut, die Kommunikation erfolgt über die Internetverbindung aus dem zentralen IT-Netz.
- Wenn WIFI-Netzwerke für die Steuerung drahtloser Endgeräte verwendet werden müssen, bildet das WLAN ein eigenes Subnetz ab, in dem nur definierte Geräte zugelassen werden. Für die Steuerung der Geräte werden eigens dafür vorgesehene Endgeräte verwendet. Innerhalb des WLAN wird eine separate SSID ausgestrahlt
- Innerhalb der Netze wird, wenn möglich, der 802.1x Standard implementiert, der eine Authentifizierung jedes Netzteilnehmers erzwingt.
- Kommunikation zwischen einzelnen Subnetzen erfolgt immer über eine Firewall und über definierte Ports und Protokolle.
- Das BSI empfiehlt: „Innerhalb des GA-Netzes (Gebäudeautomations-Netzes) SOLLTE eine Netzsegmentierung umgesetzt werden, die bedarfsgerecht einzelne GA-Systeme, einzelne TGA-Anlagen oder einzelne Gruppen von TGA-Anlagen innerhalb eines GA-Systems voneinander trennt.[22]
- Die Anbindung der GA an IT-Komponenten aus der Unternehmens-DMZ (Energiemanagementsystem, Mail-Relay, Alarmierungssysteme) ist immer über eine Firewall umzusetzen, GA-Netze sind von IT-Netzen zu trennen.
- Die Latenzzeiten der Kommunikation zwischen den Subnetzen, insbesondere, wenn sie über eine Firewall geroutet werden, sind bei der Konzeption zu berücksichtigen.
- Innerhalb der GLT-Netze dürfen an den Komponenten keine offenen Ports (z. B. USB, LAN) und Kommunikationsadapter (Bluetooth, WiFi) aktiviert sein.
- Wartungszugänge sollen entweder über virtuelle Desktops des Gebäudebetreibers implementiert werden oder das Operator Interface wird über die Infrastruktur des Betreibers und unter Verwendung geeigneter Authentifizierungsmaßnahmen (z. B. 2-Faktor-Authentifizierung) bereitgestellt.
- Die Kommunikation innerhalb der GLT sollte nach Möglichkeit verschlüsselt (BACnet Secure Protokoll, KNX-Secure) erfolgen
- Intrusion Detection und Intrusion Prevention Systeme (IDS/IPS) an der zentralen Firewall erkennen verdächtige Aktivitäten und können diese unterbinden. Sie können den Datenverkehr innerhalb der OT-Netze und zwischen IT- und OT-Netzen überwachen und erkennen unbekannte Netzteilnehmer und Protokolle.

[22] „INF.14 Gebäudeautomation (Edition 2023)“, 01.02.2023 [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_14_Gebaeudeautomation_Edition_2023.html

5.2 ICS-Monitoring (Industrial Control System Security)

In der Industrie sind Systeme zum Monitoring der Operational Technology verbreitet. Grundsätzlich können diese Systeme auch für das Monitoring der GA-Netze und ihrer Komponenten verwendet werden.

Wesentliche Funktionen dieser Lösungen sind:

- Automatische Erkennung und Inventarisierung der Netzkomponenten und Identifizieren der Kommunikationsbeziehungen
- Erkennung von Schwachstellen und Generierung von Reports
- Integrierbar in SOC, SOAR, SIEM
- Anomalie Erkennung (Fremde Netzteilnehmer, fremde Kommunikationsprotokolle)
- Auslösen von Alarmen nach definierbaren Regeln und Parametern
- Aufzeichnen der Historie von Asset-Änderungen, Generierung von Reports

Weitere Produkte zur IT-Sicherheit in OT/FM

- SOAR (Security Orchestration, Automation and Response) ist eine Kombination aus kompatiblen Programmen, die es einem Unternehmen ermöglicht, aus unterschiedlichsten Quellen Daten über Sicherheitsbedrohungen einzusammeln.
- SIEM (Security Information and Event Management) kombiniert die zwei Konzepte Security Information Management (SIM) und Security Event Management (SEM) für die Echtzeitanalyse von Sicherheitsalarmen aus Anwendungen und Netzwerkkomponenten. SIEM dient damit der Computersicherheit einer Organisation und ist ein Softwareprodukt, das zentral installiert oder als Cloud-Service genutzt werden kann.

[19] „Zertifizierung BSI“, 15.01.2025 [Online]. Available: www.bsi.bund.de/zertifizierung

5.3 Überprüfung der Maßnahmen

Die Wirksamkeit der getroffenen Maßnahmen kann am ehesten durch Externe unter realen Bedingungen überprüft werden.
Sollte es zu einem Vorfall kommen, ist ein geeigneter Dienstleister, der die notwendige Intervention beherrscht, von Vorteil. Optimalerweise ist der Dienstleister bereits im Vorfeld mit der Aufgabe der Digital Forensics and Incident Response (DFIR), also der Notfallübernahme, betraut worden. Auch sollte der Dienstleister im Vorfeld in etwaige Übungen und methodische Überprüfungen (Red, Purple und Blue Teaming) eingebunden sein. Eine Notfallnummer sollte physisch, wie auch bei Feuerwehr-Hinweisschildern, gut sicht- und erreichbar dokumentiert werden.

Die größten Schäden bei Cyberangriffen entstehen durch verspätete Meldung und Einleitung von Maßnahmen.

5.4 Erforderliche Rollen und Prozesse (Aufbau-/ Ablauforganisation)

Um die Cybersicherheit im FM zu gewährleisten, müssen die verschiedenen Rollen im FM, in der IT und Nutzer/Mieter eng zusammenarbeiten und die relevanten Prozesse aufeinander abgestimmt werden. Es ist wichtig, dass jede Rolle ihre spezifischen Aufgaben und Verantwortlichkeiten versteht und dass es klare Prozesse gibt, um die Cybersicherheit zu gewährleisten.

Grundsätzlich haben alle Beteiligten die Verantwortung, sich an unternehmensinterne Prozesse und Kommunikationswege zu halten, um keine unbewussten Einfallstore für externe Angriffe zu öffnen.
Hierzu zählt auch die Beschaffung von Software durch Anwender oder die FM-Abteilung ohne Einbindung der IT-Abteilung oder eine konsequente Zulieferung der Informationen im Rahmen einer IT-Software-Inventur.
In den definierten Prozessen und deren Implementierung sind Aspekte wie eindeutige Verantwortlichkeiten, organisatorische Schnittstellenabgrenzung, die Befähigung von Mitarbeitern und Maßnahmen zur Vermeidung eines Organisationsverschuldens wichtig und zu berücksichtigen.

Bezogen auf die beteiligten Rollen ist der Facility Manager verantwortlich für die Sicherheit der Gebäudeinfrastruktur, einschließlich der physischen und digitalen Aspekte. Er muss sicherstellen, dass alle Systeme und Geräte sicher sind und den neuesten Sicherheitsstandards entsprechen. Zudem ist er für die Klärung von Schnittstellen zuständig, insbesondere in Smart Buildings, die eine Vielzahl von Verbindungen zu Energieversorgern oder anderen Gebäuden aufweisen und dadurch Teil intelligent vernetzter Smart Cities werden.
Ein weiterer wichtiger Aspekt seiner Arbeit ist die Schulung des Personals in Bezug auf Sicherheitsprotokolle und Notfallmaßnahmen.

Externe FM-Dienstleister und operative Techniker unterstützen den Facility Manager, indem sie Wartungs- und Reparaturarbeiten an sicherheitsrelevanten Systemen durchführen. Sie berücksichtigen dabei die Sicherheitsmaßnahmen von IT und FM beim Einbau neuer oder Austausch alter Geräte. Zudem dokumentieren sie ihre Arbeiten und benachrichtigen die IT-Abteilung über durchgeführte Maßnahmen. Sicherheitsvorfälle und -schwachstellen melden sie an den Facility Manager und die IT-Abteilung.

Die IT-Abteilung, insbesondere der IT-Sicherheitsmanager, spielt eine zentrale Rolle bei der Verwaltung und dem Schutz der digitalen Infrastruktur, einschließlich Netzwerken, Servern und Datenbanken. Der IT-Sicherheitsmanager ist verantwortlich für die Identifizierung und Bewertung von Sicherheitsrisiken im Zusammenhang mit der Gebäudeinfrastruktur. Er implementiert Sicherheitsmaßnahmen, einschließlich der Aktualisierung von Systemen und Software, der Implementierung von Firewalls und anderen Sicherheitswerkzeugen und der Durchführung regelmäßiger Sicherheitsüberprüfungen. Zudem muss er sich mit Organisationsverschulden auseinandersetzen, das sich auf eine unzureichende Organisation bezieht, die zu einem Schaden führt. Im Bereich der IT-Sicherheit kann dies beispielsweise mangelndes Risikomanagement, schlechte Passwortsicherheit, fehlende Datensicherungen oder unzureichende Notfallpläne umfassen.

Die Nutzer und Mitarbeiter der Immobilie sind ebenfalls ein wichtiger Bestandteil der Cybersicherheit. Sie müssen die festgelegten Sicherheitsprotokolle und -richtlinien einhalten und verdächtige Aktivitäten oder Sicherheitsvorfälle an die zuständigen Abteilungen melden. Ihre Teilnahme an Schulungen und Weiterbildungen zum Thema Cybersicherheit ist essenziell, ebenso wie der verantwortungsbewusste Umgang mit sensiblen Informationen und Zugangsdaten. Jeder Mitarbeiter sollte genau wissen, was seine Aufgaben und Verantwortlichkeiten in Bezug auf die Cybersicherheit sind. Dies unterstreicht die Notwendigkeit, die Verantwortlichkeiten klar zu definieren und an die entsprechenden Rollen zu delegieren.

Zusammen tragen diese Rollen und ihre spezifischen Aufgaben dazu bei, die Cybersicherheit in einer Immobilie zu gewährleisten und potenzielle Bedrohungen zu minimieren. Prozesse wie die Risikobewertung, die Implementierung von Sicherheitsmaßnahmen und die regelmäßige Schulung der Mitarbeiter sind entscheidend, um ein hohes Sicherheitsniveau aufrechtzuerhalten. Die Klärung von Schnittstellen, insbesondere in Smart Buildings, ist ebenfalls von großer Bedeutung, um sicherzustellen, dass alle Verbindungen sicher sind und keine Schwachstellen aufweisen.

6 Fazit

In diesem White Paper wurden die wesentlichen Erkenntnisse und Empfehlungen zum Thema Cybersicherheit für das Facility Management zusammengefasst. Es wird aufgezeigt, dass die Cybersicherheit von entscheidender Bedeutung ist und sowohl technische als auch organisatorische Maßnahmen erfordert, um die Sicherheit von Gebäuden und deren Infrastrukturen zu gewährleisten.
Die zunehmende Vernetzung und Digitalisierung im FM bringen sowohl Chancen als auch Herausforderungen mit sich. Präventive Maßnahmen, regelmäßige Sicherheitsüberprüfungen und Schulungen für Mitarbeitende sind unerlässlich, um Gebäude sicher und betriebsfähig zu halten.
Die IT-Sicherheit in der Gebäudeinfrastruktur ist eine kritische Aufgabe. Sie umfasst die Identifizierung und Bewertung von Risiken sowie die Implementierung effektiver Sicherheitsmaßnahmen. Der IT-Sicherheitsmanager spielt hier eine zentrale Rolle, ebenso wie die Schulung der Mitarbeiter, die oft das erste Ziel von Cyberangriffen sind.

Eine klare Definition der Verantwortlichkeiten ist unerlässlich, um die Cybersicherheit aufrechtzuerhalten und Organisationsverschulden zu vermeiden. Der aktuelle Zustand der IT-Sicherheit in vielen Gebäuden ist unzureichend, was durch Kostendruck und mangelnde praktische Umsetzung und Erfahrungen verstärkt wird. Die Zusammenarbeit mit der klassischen IT ist zwingend notwendig, wodurch bewährte Methoden auch im Facility Management anwendbar werden.
Angesichts der hohen Wahrscheinlichkeit erfolgreicher Angriffe ist es entscheidend, proaktiv und nachhaltig Maßnahmen zur IT- und Cybersicherheit zu ergreifen. Nur so können potenzielle Schäden frühzeitig erkannt und verhindert werden.
Die Cybersicherheit im FM erfordert eine kontinuierliche Anpassung und Verbesserung der Sicherheitsstrategien. Durch die Nutzung bestehender IT-Erfahrungen und die Implementierung präventiver Maßnahmen können Gebäude und ihre IT- und OT-Infrastrukturen effektiv geschützt werden, wodurch ein sicherer Betrieb ermöglicht werden kann.

[19] „Zertifizierung BSI“, 15.01.2025 [Online]. Available: www.bsi.bund.de/zertifizierung

7 Literaturverzeichnis

[1] Kevin Wennemuth, CID GmbH, 2024

[2] „www.statista.com“, 15.01.2025 [Online].
Available: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

[3] g. &. Lünendonk, GEFMA 945: CAFM-/IWMS-Trendreport 2023, 2023

[4] „Digital Operational Resilience Act (DORA)“, 15.01.2025 [Online].
Available: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

[5] „TIBER-DE“, 07.02.2025. [Online].
Available: https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/tiber-de/tiber-de-816986

[6] „Eu Cyber Security Act“, 15.01.2025 [Online].
Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/Cyber-Security-Act/cyber-security-act.html

[7] „NIS2-Richtlinie“, 15.01.2025 [Online].
Available: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L1148

[8] „BSI-Grundschutzkataloge“, 15 01 2025 [Online].
Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.htm

[9] „BSIG-, BSI-, IT-Sicherheitsgesetz“, 15.01.2025 [Online].
Available: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html; C5-Zertifizierung (Cloud Computing Compliance Criteria Catalogue)

[10] „IT-Sicherheitsgesetz (IT-SiG)“, 15.01.2025 [Online].
Available: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

[11] „Datenschutz-Grundverordnung (DSGVO)“, 2016 [Online].
Available: https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/it-digitalpolitik/datenschutz/datenschutzgrundvo-liste.html

[12] „ISO/IEC 27001“, 15.01.2025 [Online].
Available: https://cyberzoni.com/standards/iso-27001

[13] „IEC 62443“, 15.01.2025 [Online].
Available: https://www.dke.de/de/arbeitsfelder/industry/iec-62443-cybersecurity-industrieautomatisierung

[14] „GMBI, Nr. 25“, 11.2022 [Online]. Available: https://baua.de

[15] „TRBS 1115, Teil 1“, 15.01.2025 [Online].
Available: https://www.baua.de/DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1

[16] „KRITIS-Verordnung (BSI-KritisV)“, 15.01.2025 [Online].
Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KM4/KRITIS-Dachgesetz.html

[17] „NIS-Richtlinie“, 15.01.2025 [Online].
Available: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

[18] „BSI – Cloud Security“, 15.01.2025 [Online].
Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/C5_Aktuelle-Version/C5_AktuelleVersion_node.html

[19] „Zertifizierung BSI“, 15.01.2025 [Online].
Available: www.bsi.bund.de/zertifizierung

[20] „Cyberangriffe auf Aufzüge“, 15.01.2025 [Online].
Available: https://www.tuvsud.com/de-de/branchen/real-estate/technische-gebaeudeausruestung-und-aufzuege/aufzuege-fahrtreppen-foerdertechnik/aufzug-cybersicherheit

[21] „BACnet Committee“, 07.02.2025 [Online].
Available: https://bacnet.org/

[22] „INF.14 Gebäudeautomation (Edition 2023)“, 01.02.2023 [Online].
Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/10_INF_Infrastruktur/INF_14_Gebaeudeautomation_Edition_2023.html

[23] „EU-Rechtsakt zur Cyberresilienz“, 15.01.2025 [Online].
Available: https://digital-strategy.ec.europa.eu/de/policies/cyber-resilience-act

8 Abbildungs- und Tabellenverzeichnis

Abbildung 1: Zusammenhang der Begriffe der Informationssicherheit[1] 4
Abbildung 2: Übersicht weltweiter Cyberangriffe pro Jahr[2] 8
Abbildung 3: Aktuelle Herausforderungen für die Budgetplanung der Anwender[3] 10
Abbildung 4: Übersicht über ISO 2700x und IEC[1] 18
Abbildung 5: Detaillierte Übersicht über die IEC[1] 19
Abbildung 6: KRITIS-Verordnung (BSI-KritisV) 21
Abbildung 7: EU-NIS-Richtlinie/NIS-2-Richtlinie 22
Abbildung 8: Wesentliche Maßnahmen[1] 29

[1] Kevin Wennemuth, CID GmbH, 2024
[2] „www.statista.com“, 15.01.2025 [Online]. Available: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
[3] g. &. Lünendonk, GEFMA 945: CAFM-/IWMS-Trendreport 2023, 2023

Die Erarbeitung des White Papers erfolgte durch die Autoren
Thomas Kalweit, Matthias Mosig, Marko Opic, Maik Schlundt, Holger Voß, Kevin Wennemuth

Erstellt am: 15.10.2025

Das White Paper wurde vom gefma Arbeitskreis Digitalisierung unter Vorsitz von Matthias Mosig bestätigt.

Herausgeber:
gefma e. V.
Deutscher Verband für Facility Management e. V.
Basteistraße 88
53173 Bonn, Germany
Tel. +49 228 850276-0
info@gefma.de
www.gefma.de

Verantwortliches Gremium:
gefma Arbeitskreis Digitalisierung

White Paper GEFMA 944
Version 1.0/2025-10