Whitepaper

Basis-Cybersicherheit in vernetzten Gebäuden

Handlungsoptionen und Orientierungshilfen

Version 2.0 – Stand Februar 2022*
Verband der Elektro- und Digitalindustrie

* Cybersicherheit ist ein sich schnell entwickelndes Thema.
Die Positionierung des ZVEI wird daher kontinuierlich weiterentwickelt.

Inhalt

Vorwort 2

1. Cybersicherheit im Gebäude: “Herausforderungen und geteilte Verantwortlichkeiten” 4

2. Anwendungsbereich: Vernetztes Gebäude im Umfeld der Digitalisierung 7

3. Vernetzung und Digitalisierung in Home & Building 9

4. Generisches Architekturbild: Anwendungsbereiche in der Gesamtbetrachtung 11

5. Risikoanalyse 16

6. Grundlegende Risiken für das vernetzbare Gebäude 21

7. Basis-Cybersicherheitsmaßnahmen 24

8. Fazit 28

Anhang 1: Orientierungshilfen für weitere Recherchen 30

Anhang 2: Erläuterungen wichtiger Grundbegriffe 32

ZVEI: Der Verband der Elektro- und Digitalindustrie 33

Vorwort

Die Covid19-Pandemie hat in vielen Bereichen enorme Veränderungen angestoßen und deutliche Auswirkungen auf das Leben, Wohnen und Arbeiten mit sich gebracht. Eine der zentralen Prozessveränderungen im Arbeitsleben, gerade hinsichtlich des Umfangs der Nutzung, ist die enorme Zunahme der Bedeutung des Homeoffice. Vor dem Hintergrund weltweiter CO_2-Reduktionsziele ist zu erwarten, dass dieser Trend auch über die Krise hinaus andauern wird. Mit einer Verlagerung der Arbeitstätigkeit in die „eigenen vier Wände“ hat aber auch eine Verschiebung der Cyber-Angriffe und eine Re-Fokussierung auf das Angriffsziel „Home“ stattgefunden. Es ist zu vermuten, dass eine Welle von Schadprogrammen aus dem Homeoffice in die Unternehmen getragen werden.[1]

Ein wesentlicher Treiber ist die Digitalisierung im Bereich Smart Home und die fortschreitende Vernetzung im Bereich Smart Building. So stellt sich der Home-Sektor als Bereich mit höchster IoT-Durchdringung dar. Dieses kann im Digitalisierungsindex und in Zahlen zur IoT-Nutzung abgelesen werden [2]. Dieser Trend wird sich weiter verstärken, besonders auch dadurch, dass nur mit einer intelligenten Gebäudeautomation die enormen Potenziale zur nachhaltigen Effizienzsteigerung und damit die Einsparung von CO_2-Emissionen von Gebäuden genutzt werden können.[3]

Auch den gesellschaftlichen und demographischen Veränderungen (Alterspyramide), z. B. die Zunahme der Personen mit Pflegbedürftigkeit, welche in ihren eigenen vier Wänden verbleiben wollen, kommt eine immer größere Bedeutung bei der Smart-Home-Nutzung zu.

Dabei besitzt der deutsche Markt die Besonderheiten einer niedrigen Wohneigentumsquote von ca. 51 Prozent, jedoch einem hohen Anteil an Einfamilienhäusern (ca. 16 Mio.) [4] und präsentiert sich somit als Mietermarkt.

[1] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html
[2] https://www.digitalisierungsindex.de / https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-download-Langfassung-digitalisierungsindex-2020.pdf?__blob=publicationFile&v=4
[3] https://www.zvei.org/fileadmin/user_upload/ZVEI-Plattform_Gebaeude_Forderungen_zur_Bundestagswahl_2021_Juli_2021_neu.pdf
[4] Wohneigentumsquote in Europa | Statista, https://de.statista.com/statistik/daten/studie/39010/umfrage/bestand-der-einfamilienhaeuser-in-deutschland-seit-2000

Im Bereich der Nicht-Wohngebäude weist Deutschland eine hohe technische Ausstattungsquote auf. Daraus resultiert ein hoher Vernetzungsgrad und eine entsprechende Servicelandschaft.

Diese Aspekte müssen bei der Betrachtung der Informationssicherheit eines Gebäudes und seiner Systeme berücksichtigt werden. Durch die Anzahl und Heterogenität der Akteure ist die Adressierung der jeweiligen Verantwortlichkeiten eine besondere Herausforderung, die Aufteilung der verschiedenen Funktionalitäten erfordert daher zwangsläufig eine Koordination, um ein adäquates Informationssicherheitsniveau zu erreichen.

Diesen Herausforderungen trägt der ZVEI Rechnung, indem er diese Themen in der Plattform Gebäude bündelt, und insbesondere auch durch die “Task Force Cybersicherheit im Gebäude”. Mit diesem Whitepaper soll zum einen Gebäudebesitzern oder Betreibern eine erste Orientierung in diesem komplexen und dynamischen Umfeld gegeben werden. Zum anderen soll es den Verantwortlichen in den Unternehmen (Produktmanagement, Prozessentwicklung, Forschung und Entwicklung und Unternehmensführung) frühzeitig in der Entscheidungskette zu Produkten bei der Betrachtung des Themas Cybersicherheit helfen.

1. Cybersicherheit im Gebäude: “Herausforderungen und geteilte Verantwortlichkeiten”

Vernetzung und Digitalisierung sind ohne Cybersicherheit in Produkten und Anwendungen nicht zu gestalten. Das ist das Selbstverständnis der im ZVEI organisierten Herstellerunternehmen. Mehr noch ist es der gemeinsame Anspruch, dass Cybersicherheit zu einem selbstverständlichen Bestandteil der Produkt-, System- und Servicequalität wird. Vor diesem Hintergrund besteht Handlungsbedarf. Die ZVEI-Mitglieder skizzieren mit dem vorliegenden Whitepaper Überlegungen zur Weiterentwicklung, zum Stand der Technik, zu Prozessen und Organisationsstrukturen. Dies ist wichtig und dringlich, denn Cybersicherheit ist eine zentrale Grundlage für das Kundenvertrauen, das Funktionieren von Geschäftsprozessen und einer sich weiter digitalisierenden Gesellschaft als Ganzes. Das Whitepaper steht vor diesem Hintergrund für das klare Commitment der ZVEI-Mitgliedsunternehmen, den bereits begonnenen Weg entschlossen fortzuführen. Viele Maßnahmen wurden bereits in Produkten und Anwendungen umgesetzt. Doch sollte die Cybersicherheit kontinuierlich weiterentwickelt werden. Diese Weiterentwicklung kann jedoch nur übergreifend als „gemeinsame Verantwortung“ von allen Akteuren erfolgen. Mehrere Grundprinzipien müssen dabei berücksichtigt werden:

Cybersicherheit ...

1. wird integraler Bestandteil von vernetzten Produkten, Systemen und Services werden;
2. muss angesichts der dynamischen Entwicklung des Risikoumfelds (Cybersicherheit als „Moving Target“) flexibel und stets risikobasiert gestaltet werden;
3. umfasst den gesamten Lebenszyklus eines Produkts, das heißt die Entwicklung, Fertigung, Inbetriebnahme, den Betrieb und die Außerbetriebnahme eines Produkts und kann nicht auf *Security-by-Design* reduziert werden;
4. muss entsprechend in geteilter Verantwortung entlang des Produktlebenszyklus gemeinsam und durchgängig von Herstellern, Integratoren, Errichtern, Betreibern und Nutzern angegangen werden.

Die europäischen und internationalen Exportmärkte bilden zudem den natürlichen Bezugsrahmen für die Weiterentwicklung der Cybersicherheit. Nationale Sonderwege

sind keine Alternative und können die Wettbewerbsfähigkeit der Unternehmen gefährden. Viel eher sind durch einen gemeinsamen internationalen Dialog Kompatibilität, Interoperabilität und Innovationsmöglichkeiten zu stärken. Gemeinsam werden die ZVEI-Mitglieder die Herausforderungen der Cybersicherheit meistern. Sie setzen dabei auf europäische Ansätze, wie sie mit dem EU Cybersecurity Act, dem delegierten Rechtsakt zu Art. 3 (3) d/e/f der Funkanlagenrichtlinie, besonders aber einer horizontalen Produktregulierung im etablierten Rahmen der europäischen Produktsicherheitsgesetzgebung, dem New Legislative Framework, möglich werden. Es bedarf einer konsistenten europäischen Adressierung, die Anforderungen kohärent, effizient und effektiv umsetzbar macht. Dabei darf die internationale Anschlussfähigkeit nicht außer Acht gelassen werden. Gerade, da sich andere Weltregionen, z. B. China und die USA, ebenfalls intensiv mit der Verregelung auseinandersetzen.

- Dabei gilt es die folgenden Herausforderungen zu berücksichtigen: Besonders in gemieteter Infrastruktur stellt sich das Zusammenspiel von (z. B. von Mietern) eingebrachten Smart-Home-Produkten und der bestehenden Gebäudeinfrastruktur als Herausforderung für die Cybersecurity dar. Bei einem solchen Einsatz von entsprechenden Produkten in „geteilter Betreiberschaft“ in „halböffentlicher Infrastruktur“ nimmt die Bedeutung der Übergangsstellen nochmals zu.

- Vermieter und Investoren befinden sich häufig in einem Investitionsdilemma: Auf der einen Seite ist der Return on Investment von Digitalisierungsmaßnahmen gerade bei zu Wohnzwecken genutzten Gebäuden teilweise unklar, auf der anderen Seite können Investitionen in die Digitalisierung von Gebäuden zur Untermauerung eines Qualitätsniveaus bei Nicht-Wohngebäuden hinsichtlich Komfort, Sicherheit und Wirtschaftlichkeit genutzt werden und so die Vermietbarkeit steigern. Die politischen Diskussionen sollten zu mehr Planbarkeit bei den Investoren führen.

- Smart-Home-Produkte werden zunehmend eine immer stärkere Unterstützungsrolle für eine alternde Gesellschaft bzw. einen zunehmenden Pflegebedarf übernehmen. Dies betrifft sowohl Hilfen, die bei einem nach Heilmittelverordnung festgestellten Pflegebedarf geleistet werden könnten, als auch den gesamten Bereich des „ambient assisted living“, welches die Umsetzung von Smart-Health-Lösungen,

Lebenslaufwohnen und weiteren innovativen, die Lebensqualität verbessernden Themen ermöglicht.

- Das beschriebene Voranschreiten der „Digitalisierung“ führt zu einer Steigerung der Herausforderungen hinsichtlich der Cybersicherheit; mit der IP-Durchdringung steigt auch die Gefahr der Kompromittierung von IT-Systemen.

- Auch die voranschreitende Umsetzung einer cloudbasierten Service-Landschaft wird weitere Anforderungen stellen und Folgen haben.

- Die Herausforderung geteilter Verantwortlichkeiten, sowohl hinsichtlich der unterschiedlichen Rollen als auch in den unterschiedlichen Rollen muss beachtet werden. So wird voraussichtlich niemand alle Produkte anbieten können, die benötigt werden, um ein vollständiges Smart-Home-Umfeld zu errichten; es müssen daher Produkte von verschiedenen Herstellern betrachtet und integriert werden. Gleichzeitig gibt es im Smart-Home-Bereich nur selten Akteure, die das Gesamtsystem auch im Hinblick auf seine Verbindungen nach „außen“ im Blick haben.

- Diese Herausforderung wird zukünftig durch neue Spieler im Smart-Home-Bereich verstärkt, die ihre eigenen Geschäftsmodelle, Ökosysteme und Sicherheitsarchitekturen in den Markt bringen und damit zum einen eine faktische Normsetzungsposition übernehmen zum anderen aber nicht unbedingt die Interoperabilität mit dem restlichen Smart-Home-Umfeld im Blick haben.

2. Anwendungsbereich: Vernetztes Gebäude im Umfeld der Digitalisierung

In diesem Whitepaper werden Kritische Infrastrukturen bewusst nicht betrachtet und behandelt.[5] Wenn es um die Digitalisierung von vernetzten Gebäuden geht und damit die verbundenen global angebotenen Produkte und Lösungen adressiert werden, sollte mindestens europäisch gedacht werden. Schließlich sind diese Produkte und Lösungen weltweit verfügbar und trotzdem entsprechend den jeweiligen Regionen auszuführen, insbesondere wenn diese eine wegbereitende Funktion erfüllen. Umgekehrt sind aber auch die nationalen Anforderungen im Leitmarkt Deutschland – insbesondere an der Schnittstelle des Gebäudes zum Energiesystem – zu berücksichtigen und sollten idealerweise in Einklang mit europäischen Normen gebracht werden.

Das Whitepaper untergliedert „vernetztes Gebäude“ nicht weiter in Wohn- und Nicht-Wohngebäude beziehungsweise in „Smart Home“ und „Smart Building“. Für die Passagen, in denen doch auf die Begriffe Home und Building Bezug genommen wird, stützt sich das Papier auf die Begriffsbeschreibung der DKE Roadmap Smart Home + Building.[6] Der Begriff vernetztes oder vernetzbares Gebäude wird an dieser Stelle als Sammelbegriff für beide Gebäudetypen verwendet.

Die Betrachtung der Cybersicherheit gemeinsam für beide Gebäudetypen erleichtert die Standortbestimmung. Auch wenn sich die Verantwortungsrollen, Kompetenzen und Rechtsgrundlagen im Wohn- und Nicht-Wohngebäude unterscheiden, gibt es doch gemeinsame Ansatzpunkte und Abwägungen im Hinblick auf die Cybersicherheit. Vereinfacht geht das Whitepaper davon aus, dass in einem vernetzten Gebäude sowohl direkt als auch indirekt mit dem Internet verbundene Endgeräte installiert sein können. Zudem wird angenommen, dass alle vernetzten Gebäude folgende Gewerke umfassen, wenn auch in unterschiedlicher Ausprägung:

- Heizung, Lüftung, Wasser und Klimatisierung
- Beleuchtung und Elektroinstallation
- Energiesysteme und -steuerung
- Komfort und Entertainment
- Sicherheitstechnik und technische Überwachungssensorik
- Small Office Home Office (SOHO)

[5] https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html
[6] https://www.dke.de/resource/blob/778214/6ec4d037024b61a63d14544d181c638a/deutsche-normungs-roadmap-smart-home---building--version-2-0-data.pdf

- Hausgeräte[7]

Für die betroffenen Gewerke sollte einzeln für sich und im Verbund als System eine Betrachtung der Cybersicherheit erfolgen. Die Zusammenfassung von Wohn- und Nicht-Wohngebäude kann auf dem Niveau der Basis-Cybersicherheit, worum es in diesem Whitepaper ausschließlich gehen soll, ohne maßgebliche Verluste erfolgen.

[7] Hausgeräte werden nur insoweit betrachtet, wie sie im Zusammenhang mit der jeweiligen Kopplung mit der Gebäudeinfrastruktur/den IT-Systemen stehen.

3. Vernetzung und Digitalisierung in Home & Building

Vernetzung und Digitalisierung finden in vernetzten Gebäuden auf mehreren Ebenen statt. Missverständlich werden die Begriffe jedoch meist unscharf im Kontext von „Smart Home“ und „Smart Building“ gebündelt. Diesem Whitepaper liegt folgende Unterscheidung zu Grunde:

Digitalisierung: Analoge Daten werden digitalisiert. Zusätzlich werden analoge und/oder digitalisierte Daten über Bereitstellung, Verarbeitung, Visualisierung und Speicherung nutzbar gemacht.

Vernetzung: Dinge und Daten (digital und analog) werden miteinander verbunden, die vorher nicht miteinander verbunden waren.

Die Vernetzung kann unterschiedliche Ausprägungen haben. Aus Sicht der Cybersicherheit sind vor allem die Zugriffsmöglichkeiten und daher die indirekte oder direkte Verbindung mit dem Internet ein entscheidender Parameter für die Einschätzung. Vor diesem Hintergrund erscheint eine grobe Unterscheidung zwischen

- rein lokalen Informationsaustausch (z. B. Installationssysteme),
- lokalen Informationsstrukturen mit Ankopplung an das Internet
    - z. B. Punkt-zu-Punkt (weiße oder braune Ware) und
- direkter Internet-Vernetzung (z.B. IoT Geräte oder Kommunikationsgeräte wie Mobiltelefone und Tablets) sinnvoll.

Kommunikationsgeräte und -systeme, welche auf offenen Kommunikationsmedien aufsetzen (z.B. Wi-Fi, RF, sonstige Funknetze, Powerline), müssen entsprechend ihrer Eigenschaften berücksichtigt werden. Der hierbei öffentliche Zugriff auf die Informationsübertragung erfordert entsprechende Berücksichtigung auf der Kommunikationsebene und kann auch auf Daten und/oder Anwendungsebene kompensiert werden.

Digitalisierung und Vernetzung wirken sich zusammen direkt auf die Cybersicherheit von vernetzten Gebäuden und den darin enthaltenen Produkten aus. Die Angriffsmöglichkeiten vermehren sich und Angriffe skalieren viel schneller im Gebäude und dem gesamten Internet der Dinge. Das heißt, viel mehr Geräte und Systeme können in kürzerer Zeit von Angriffen auf die Cybersicherheit betroffen sein. So

machen Cyberangriffe auch nicht mehr vor Domänengrenzen halt, da sich diese im Zuge der Vernetzung zusehends vermischen. Umso wichtiger ist es, übergreifende grundlegende Anforderungen und Maßnahmen für Cybersicherheit zu definieren. Somit kann jedes Produkt, System und Gewerk seinen fähigkeits- und risikobasierten Beitrag leisten, so dass in Summe Cybersicherheit im Gebäude entsteht.

Die fortschreitende Digitalisierung und Datenverarbeitung werden zunehmend Anwendungen ermöglichen, die über eine reine Vernetzung von Geräten hinausgehen. Bei der Sicherheitsbetrachtung muss daher differenziert in einem mehrstufigen Verfahren (hinsichtlich Produktintegration) die notwendige Sicherheit umgesetzt werden, welche von den Anwendungen und Diensten aus regulatorischer Sicht und aus Endanwendersicht gefordert werden.

Eine direkte Übertragung der Gesamtanforderungen an alle in der Diensterbringung beteiligten Geräte und Systeme ist nicht praktikabel und auch nicht zielführend. Die benötigte Systemsicherheit in einem vernetzten Home und Building muss in einem mehrstufigen Verfahren in einer Risikoanalyse für die beteiligten Komponenten bewertet werden. Dies ist notwendig, um geeignete Maßnahmen treffen zu können.

Bei Änderungen im Lebenszyklus[8] des Gesamtsystems muss auf jeder veränderten Bedrohungssituation mit einer neuen Risikobewertung Rechnung getragen werden.

[8] Die Nutzungsdauer im Kontext von Gebäuden ist nicht direkt vergleichbar mit der von Konsumgütern. Typischerweise ist die von Gebäuden längerfristig. Weiterhin haben Infrastrukturen unterschiedliche Nutzungs- und Laufzeiten als die Dienste.

4. Generisches Architekturbild: Anwendungsbereiche in der Gesamtbetrachtung

Grundsätzlich hat Cybersicherheit den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Dingen und Daten angesichts zahlreicher Bedrohungen sicherzustellen. Diese drei Schutzziele stellen das Grundgerüst jeder Sicherheitsbetrachtung dar. Für das vernetzte Gebäude skizziert dieses Whitepaper drei Bedrohungen, die die Cybersicherheit maßgeblich beeinflussen: Die Modifizierung der Anwendungssoftware, der unberechtigte Zugriff auf ein Produkt und die Verletzung der Privacy (siehe Kapitel 5).

Ausgangspunkt für die Betrachtung der Bedrohungen und der Cybersicherheit ist ein generisches Architekturbild eines vernetzten Gebäudes. Klar ist, dass solch ein Architekturbild auch beliebig anders aufgebaut werden kann, beziehungsweise in der Realität anders umgesetzt wird.

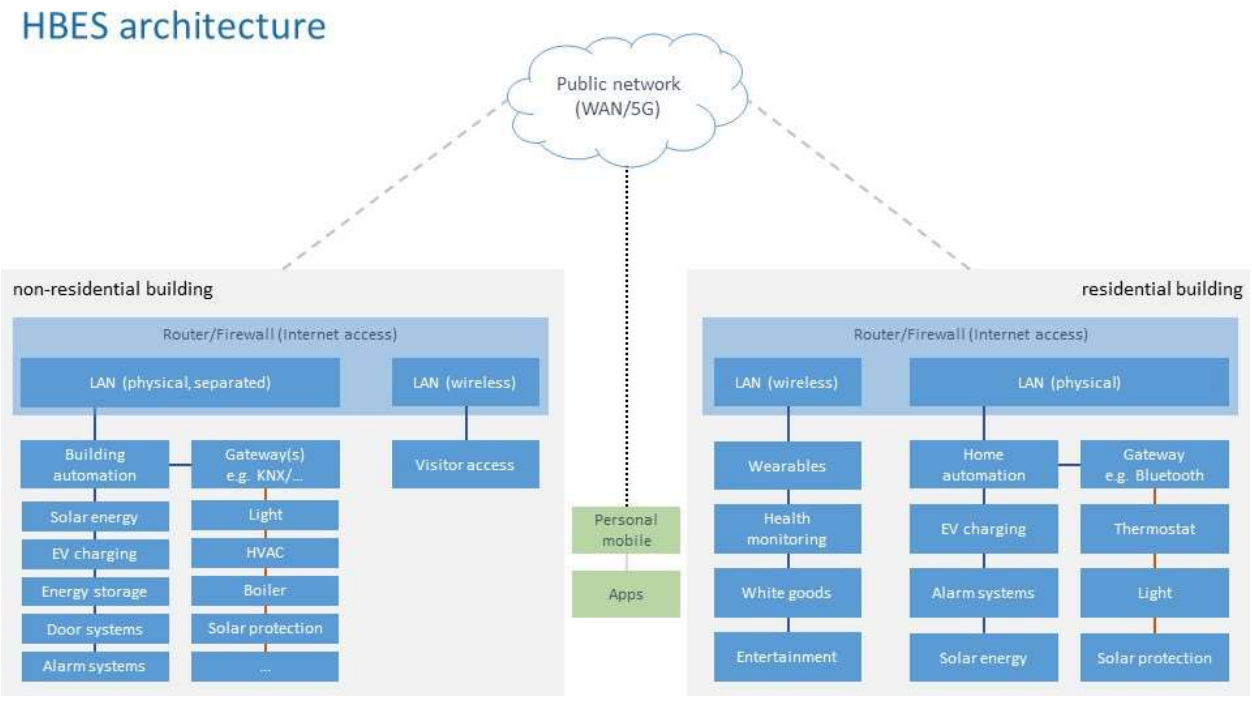

Abbildung 1: Architekturvarianten (vereinfacht) für eine informationstechnische Anbindung eines Home and Building Electronic Systems (HBES)[9]

Anhand der unterschiedlichen Möglichkeiten einer informationstechnischen Anbindung (Architekturvarianten) lassen sich mindestens fünf zentrale Punkte feststellen, die im Hinblick auf die Cybersicherheit adressiert werden müssen. Selbstverständlich ist

[9] Non-residential building: Entsprechend unserer Vorbemerkung in Kapitel 2 sind hier kritische Infrastrukturen, an deren Gebäude besondere Anforderungen gestellt werden könnten, ausgenommen.

diese Auflistung nicht als vollständig oder umfassend anzusehen. Sie soll eine erste Orientierung bieten, kann aber eine dezidierte Sicherheitsbetrachtung nicht ersetzen:

1) Die Geräte mit direkter Verbindung zu Internet und Mobilfunk, z.B. Geräte, die über einen eigenen Netzzugang oder ein Funkmodul verfügen.
2) Router als zentrale „Gateways“ zu den Geräten und Systemen im Gebäude.
3) Die Punkt-zu-Punkt-Verbindung von Haushaltsgeräten mit Mobiltelefonen, Tablets etc., wodurch eine indirekte Verbindung mit Internet und Mobilfunk entsteht.
4) Gateways und sonstige Übergänge zur Gebäudeinfrastruktur und fest verbauten Installationssystemen.
5) Über das Internet angebundene Backendsysteme.

Die unterschiedlichen Architekturvarianten wie in Abbildung 1 dargestellt sind in ihrer technischen Umsetzung was Daten, Anwendungen und Kommunikationsprotokolle betrifft sehr unterschiedlich. Um hierbei eine Unterscheidung vornehmen zu können, hilft es, die Informationsebene von der Anwendungsebene und der Kommunikationsebene abzugrenzen. Das “Home and Building Architecture Model Framework” gruppiert die entsprechenden Gewerke und gliedert die technischen Aspekte anhand ihrer Datenintegration in Zonen.

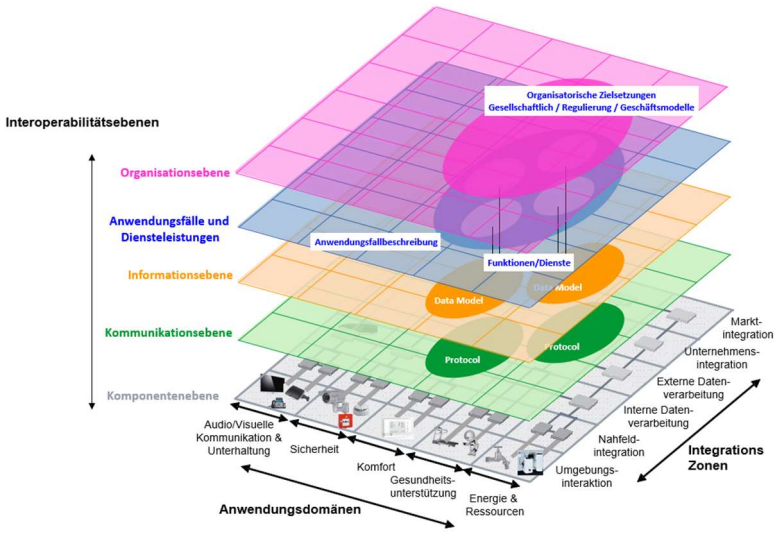

Abbildung 2: Das Heim und Gebäude Modell-Framework[10]

Das Heim und Gebäude Modell-Framework (Abbildung 2) beschreibt die einem Endverbraucher zugeordneten Themenbereiche aus dem Blickwinkel der Standardisierung. Der Endverbraucher wird bei dieser Betrachtung in den Mittelpunkt

[10] Das Bild ist in Anlehnung an die Referenzarchitektur für Industrie 4.0 erstellt worden. https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/rami40-einfuehrung-2018.html / https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf

gestellt und das Ökosystem um ihn herum aufgebaut. Es stellt keine Vorgabe für IT-Architekturen dar, sondern beschreibt und modelliert die Komplexität in einem Heim und Gebäude. Ebenso stellt es die unterschiedlichen Themenbereiche/Gewerke in Zusammenhang.

Gerade im Hinblick auf eine differenzierte Umsetzung von Sicherheitsanforderungen lassen sich interoperable Systeme modellieren, die aus technischer Sicht interagieren können, aber eine Skalierung bezüglich des Datenzugriffs und Verwendung erlauben. Diese differenzierte Betrachtung ist notwendig, um eine statische Cybersicherheitsumsetzung zu vermeiden und eine flexible anwendungsbezogene Umsetzung zu ermöglichen.

Technologietrends:

- IP-basierte Netzwerkstruktur wird dominant. Die gemeinsam genutzte IP-Infrastruktur ermöglicht eine Kopplung zwischen Systemen unterschiedlicher Domänen bis hin zu Cloud Funktionalitäten. Konfiguration, Betrieb und Wartung erfolgen auf IP basierten Systemen.
- Die IP-Infrastruktur ist erst der halbe Weg zur Durchgängigkeit aller Anwendungen; zwingende Voraussetzung zur einfachen Verknüpfbarkeit ist semantische Interoperabilität – semantisches Interworking – auf Anwendungsebene. Semantisches Interworking bedeutet die Integration unter Nutzung von gemeinsamen Information Modeling bzw. Ontologien und damit Koexistenz der Technologien sowie gemeinsame Technologie Repräsentation mit konfigurierbarem und erweiterbarem Mapping auf abstrahierter Ebene.
- Die Einbindung der digitalen Abbilder (Digital Twin) in eine digitalisierte Gebäudeinfrastruktur (Building Information Modeling – BIM)

Funktionale Trends:

- Der Trend geht zu hoher Connectivity, „Always on“ mit dem Netz verbunden sein; Connectivity ist eine Kernanforderung an nahezu alle Applikationen des Gebäudes.
- Gebäudefunktionalität und die damit verbundene technische Ausstattung steigen sowohl im Nicht-Wohngebäude als auch im Wohnbau. Das führt zu hoher technischer Anwendungsdichte. Alle Funktionen werden miteinander verknüpft.

- Gebäude werden zum Prosumer im Energienetz bis hin zu energieautarken Gebäuden.
- Vielfalt und Umfang an Serviceanbindungen wachsen.

Gesellschaftliche Trends:

- In den 19,2[11] Millionen Wohngebäuden in Deutschland nutzten 2020 etwa 37 Prozent der Bürgerinnen und Bürger mindestens eine Smart-Home-Anwendung, bei den über 50-Jährigen waren es 50 Prozent.
    - Drei Hauptbereiche stehen im Fokus: a) Energie & Klima, b) Sicherheit und c) Haus & Garten.
    - Der Bereich a) ist führend, mit Beleuchtung, Heizung, Funk-Steckdose und Verbraucherzähler, gefolgt von b)

- Das Durchschnittsalter der deutschen Bevölkerung steigt jährlich weiter an: Betrug sie 1990 noch 39,3 Jahren, lag sie 2020 bereits bei 44,5 Jahren[12]. Damit kommt der älteren Bevölkerung eine größere Bedeutung bei der Nutzung von Smart-Home-Anwendungen zu. Bei den 65-Jährigen steht die Benutzerfreundlichkeit mit 76 Prozent auf Platz eins der Anforderungen[13]. Dazu zählen:
    - benutzerfreundliche Sprachschnittstellen, sogenannte Smart Speaker
    - einfache Inbetriebnahme von Neugeräten mittels QRC-Scans
    - Wechsel von IoT zu IoTT, also the „Thinking Things“. Das sind „denkende Systeme“ mit selbstständigen bzw. autonomen Entscheidungen.

- Mit dem demographischen Wandel der Gesellschaft verlagern sich zunehmend Prozesse in den Smart-Home-Bereich, wie Pflege und Betreuung. 2019 lag die Zahl der Pflegebedürftigen in Deutschland beispielsweise bei 4,1 Millionen, Tendenz steigend[14].

[11] Quelle: Statistisches Bundesamt und eigene Berechnungen
[12] https://www.bib.bund.de/DE/Fakten/Fakt/B19-Durchschnittsalter-Bevoelkerung-ab-1871.html
[13] https://www.bitkom.org/Bitkom/Publikationen/Smart-Home-Studie-2020
[14]https://www.destatis.de/DE/Presse/Pressemitteilungen/2020/12/PD20_507_224.html#:~:text=Presse%204%2C1%20Millionen%20Pflegebed%C3%BCrftige%20zum%20Jahresende%202019&text=WIESBADEN%20%E2%80%93%20Im%20Dezember%202019%20waren,des%20Pflegeversicherungsgesetzes%20(%20SGB%20XI%20)

- Bedingt durch die COVID-19-Pandemie ist die berufliche Tätigkeit im Home-Office von vier Prozent vor der Pandemie auf 27 Prozent im April 2020 während des ersten Lockdown angestiegen und lag im Januar 2021 immer noch auf 24 Prozent[15].
    - Durch die durchschnittlich längere Aufenthaltsdauer im Home-Bereich stieg in diesem Zeitfenster die Nachfrage nach Consumer-Electronics-Produkten für den, z.B. für Entertainment und für IT-Geräte[16].

[15] https://de.statista.com/themen/6093/homeoffice/
[16] https://www.industry-of-things.de/diese-acht-trends-beherrschen-die-smart-homes-a-1041657/

5. Risikoanalyse

Cybersicherheit kann nur im Hinblick auf die vorhersehbare Verwendung der Geräte und Anwendungen und den damit einhergehenden relevanten Risiken sinnvoll gestaltet werden. Andernfalls laufen Maßnahmen ins Leere und verschwenden Ressourcen. Das heißt, es braucht immer risikobasierte Cybersicherheitsmaßnahmen. Ziel ist es, dass Schutzniveau und Aufwand in einem angemessenen Verhältnis zueinanderstehen. Im Umkehrschluss bedeutet dies, dass die Risikoanalyse der wichtigste erste Schritt einer jeden Security-Betrachtung von Produkten, Systemen oder Anwendungen ist. Hieraus leiten sich alle weiteren Schritte und Maßnahmen ab. Zudem sorgt dies für eine realistische Sicht der Dinge: Eine absolute Cybersicherheit gibt es nicht und nicht alles kann und muss hochsicher geschützt werden.

Je mehr Verwendungszwecke von vernetzten Geräten im Gebäude vorhanden sind, desto höher skaliert das Risiko bei gleichbleibender bzw. ausbleibender Erhöhung der Cybersicherheit.

Betrachtungsgegenstand der Risikoanalyse

Eine Risikoanalyse kann methodisch auf verschiedene Art und Weise vorgenommen werden. In diesem Whitepaper wird bewusst keine bestimmte Methodik herausgestellt. Wichtiger ist, dass die relevanten Aspekte einer Risikoanalyse klar sind: Was ist in einer Risikoanalyse zu bewerten? Folgende Punkte sind lediglich wichtige Schlüsselelemente einer Risikoanalyse, jedoch definitiv keine abschließende Auflistung:

- Einsatzort und Einsatzzweck des Geräts (intended use & use environment), des Systems oder der Anwendung
- verwendete Software und Software-Bibliotheken im Gerät, System oder in der Anwendung, inklusive Betriebssystem (v. a. im Hinblick auf Support und Updates) und der verwendeten Hardware-spezifischen Firmware
- Netzwerk-, Protokoll- und Kommunikationsschnittstellen und damit die Art der Vernetzung mit dem Internet und Mobilfunknetz (direkt, indirekt, getrennt etc.)
- Backend-Systeme und Services, soweit vorhanden
- Abgrenzung zu anderen Systemen und Aspekten, die nicht beeinflusst werden können

- relevante Unternehmenswerte, Schutzbedarf auch für die Anwendungsfälle für die Kunden muss noch berücksichtigt werden
- organisatorische Sicherheit entsprechend ISO/OSI-27000-Serie wie auch Produktsicherheit IEC 62443-3-4

Aufbau einer Risikoanalyse

Zu Beginn einer Risikoanalyse sind die relevanten Unternehmenswerte und -prozesse zu identifizieren und der Schutzbedarf hierfür festzulegen. Anschließend muss sondiert werden, welche Bedrohungen auf diese Werte und Prozesse einwirken können. Diese grundsätzliche Bewertung ist die Ausgangslage für die eigentliche Risikoanalyse. So wird die Eintrittswahrscheinlichkeit und Schadensauswirkung der Bedrohungen bewertet und daraus das Risiko ermittelt (Eintrittswahrscheinlichkeit x Schadensauswirkung = Risiko). Mit diesen Ergebnissen kann eine Bewertungsmatrix erstellt werden. So kann ein Risikoprofil für die relevanten Produkte erstellt werden. Am Ende entsteht eine Übersicht aller Produkte und deren Risiken in Abhängigkeit vom Einsatzort und/oder Einsatzzweck. Die Risiken selbst sind im Endergebnis klassifiziert und abgestuft. Dies kann zum Beispiel über mehrere Stufen erfolgen („hohes Risiko“, „mittleres Risiko“, „geringes Risiko“).

(„hohes Risiko“: rot, „mittleres Risiko“ gelb, „geringes Risiko: grün“).

		Eintrittswahrscheinlichkeit				
		Selten	Unwahrscheinlich	Möglich	Wahrscheinlich	Häufig
Schadenhöhe	Nebensächlich					
	Gering					
	Moderat					
	Bedeutend					
	Extrem					

Abbildung 3: Risiko Kategorisierung gemäß IEC 62443

Gegenstand dieser Risikobewertung ist ein von einem System oder Gerät zur Verfügung gestellter Dienst oder eine Funktionalität. Diese müssen bei einer Veränderung, z. B. durch eine Funktionserweiterung, wieder neu überprüft und gegebenenfalls mit veränderten Schutzmaßnahmen abgesichert werden. Ein Gerät kann im Verbund mit anderen Geräten mit einer Funktionserweiterung in einer möglichen Schadensauswirkung einer Veränderung unterworfen sein. Als Konsequenz daraus ist dann eine Gesamtbetrachtung vorzunehmen.

Hierfür sind die unterschiedlichen Schutzniveaus anhand ihrer Bedrohungssituation entscheidend. Diese Schutzniveaus definieren Schutzmaßnahmen, um einer Bedrohungssituation zu begegnen. Die hierfür erarbeitete Anwendungsregel VDE-AR-E-2849-1, welche die Schutzmaßnahmen der IEC 62443 für den Heimbereich überträgt, gibt Handlungsempfehlungen basierend auf entsprechenden Schutzniveaus anhand grundlegender Geräteeigenschaften.

#	Gegenstand	Risikoklasse	Begründung / Herleitung	Schutz-maßnahme
1	Gerät X	geringes Risiko	Gerät wird fest im Gebäude installiert und hat keine direkte oder indirekte Verbindung zum Netz	a, b, c ... mit Prio 1, 2 und 3
2	Gerät Y	mittleres Risiko	Auf dem Gerät kann Software von Drittanbietern ausgeführt werden	a, b, c ... mit Prio 1, 2 und 3
3	Gerät Z	hohes Risiko	Gerät ist über IP-vernetzt und kann Software aktiv ausführen	a, b, c ... mit Prio 1, 2 und 3

Abbildung 4: Beispielhafte Gerätebezogene Ergebnisstabelle gemäß IEC 62443

Das Ergebnis ist dann die Grundlage für die Auswahl der zu implementierenden Sicherheitsmaßnahmen und deren Skalierung. Die Maßnahmen leiten sich vom jeweiligen Risiko ab. Für die konkrete Auswahl der Maßnahmen müssen verschiedene Maßnahmenkataloge berücksichtigt werden (ISO-27000-Serie und die Maßnahmenkataloge des BSI IT-Grundschutzes[17]). Dieses Vorgehen sorgt für Effizienz und Investitionssicherheit und erleichtert die Serienpflege der Produkte.

[17] BSI Maßnahmenkataloge: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html;jsessionid=BBBD1B2D8F0AF535A38C1B8B37C4999B.1_cid351

Darüber hinaus können so weitere regulatorische Vorgaben erfüllt werden, wie

Risikoanalyse ist kein einmaliger, sondern ein kontinuierlicher Prozess. Hersteller müssen sowohl mögliche Schwachstellen als auch Security-Vorfälle für die eigenen Produkte, deren Einsatzgebiete und Zulieferkomponenten kontinuierlich verfolgen und bewerten.

Fallbeispiel: Der Hersteller X nutzt einen Software-Baustein / eine -Bibliothek des Herstellers Y in seinen Produkten. Wenn der Hersteller Y für seine Software eine Sicherheitslücke mitteilt, muss Hersteller X für sich bewerten können, inwiefern diese Sicherheitslücke ein Risiko für das eigene Produkt darstellt und welche Schutzmaßnahmen zu ergreifen sind.

beispielsweise die Produktbeobachtungspflicht im Zuge der Marktüberwachung.

Methoden für die Risikoanalyse (Beispiel)

Für die Durchführung der Risikoanalyse gibt es standardisierte Vorgehensmodelle, wie z. B. in der IEC 62443 beschrieben.

Allgemein sollte anhand der Schutzziele Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) – der sogenannten CIA-Triade – für das jeweilige Produkt oder die Anwendung immer eine Bewertung der Risiken erfolgen. Strukturierte Vorgehensmodelle wie beispielsweise STRIDE[18] helfen, gängige Angriffs- und Manipulationsmöglichkeiten von vernetzbaren Produkten und Anwendungen zu identifizieren:

- **S**poofing (nachahmen, vortäuschen einer Identität),
- **T**ampering (fälschen, manipulieren von Daten),
- **R**epudiation (abstreiten einer Handlung),
- **I**nformation Disclosure (aufdecken, veröffentlichen von Informationen),
- **D**enial of Service (Dienstverweigerung) und
- **E**levation Privilege (unzulässige Erweiterung von Rechten).

Mehrwert generiert die Risikoanalyse, wenn die Ergebnisse in den Support und die Produktentwicklung der nächsten Generation einfließen. Auf diese Weise kann „Security-by-Design“ effizient umgesetzt werden. Zudem entwickelt sich das Unternehmen für seine Kunden zu einer **lernenden Organisation.**

[18] https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)

Verankerung der Risikoanalyse in der Organisation

Zu Beginn können verschiedene Unternehmensrollen mit der Aufgabe einer Risikoanalyse betraut werden: zum Beispiel das Produktmanagement oder die Qualitätssicherung. Mittelfristig wird in Unternehmen die funktionale Abdeckung durch die Einrichtung eines entsprechenden *Product Computer Emergency Response Team* (P-CERT) erfolgen.

6. Grundlegende Risiken für das vernetzbare Gebäude

Aus Sicht der ZVEI-Mitgliedsunternehmen sind unter Berücksichtigung der skalierbaren Auswirkungen zunächst drei allgemeine Risiken für das Umfeld des vernetzbaren Gebäudes relevant – auch wenn sicherlich zahlreiche weitere Risiken bestehen:

1. Botnetze, die Geräte und Systeme beeinträchtigen und manipulieren
2. Destabilisierung des Energienetzes durch manipulierte Geräte
3. Verletzung der Privatsphäre Einzelner oder ganzer Gruppen

Diese Risiken müssen nun auf ihre eigentliche produktrelevante Ursache zurückgeführt werden. Erst dann werden sie für ein Unternehmen greifbar. Aus Sicht eines Herstellerunternehmens können die oben genannten drei Meta-Risiken zum Beispiel wie folgt heruntergebrochen werden (Auswahl, kein Anspruch auf Vollständigkeit):

zu 1: Modifizierung der Anwendungssoftware

zu 2: unberechtigter Zugriff auf und Eingriff in das Produkt

zu 3: Verletzung der Privacy

Da sich die Bedrohungssituation im Lauf der Zeit verändern kann, ist eine Lebenszyklusbetrachtung der Risiken während der Nutzung der Geräte für intelligente Dienste notwendig. Die oben dargestellten Risiken stellen die herausgestellten Anforderungen zum gegenwärtigen Zeitpunkt dar. Diese müssen auf Basis überarbeiteter Bedrohungsanalysen, z. B. denen der ENISA (European Union Agency for Cybersecurity) auf europäischer Ebene, und der betrachteten Produktgruppen und Dienstleistungen überprüft werden, um eine zielgerichtete Sicherheitsumsetzung seitens der Hersteller zu ermöglichen.

Modifizierung der Anwendungssoftware

Das erste Risiko ist die unberechtigte Modifizierung der Anwendungssoftware eines Produkts. Das Risiko besteht darin, dass die Software eines Produkts manipuliert oder sogar vollständig ersetzt wird. Die Auswirkungen können vielfältig sein. So kann bei einer erfolgreichen Manipulation das Produkt beispielsweise als Teilnehmer eines Botnetzes für kriminelle Handlungen Dritter verwendet werden (Ransomware). In der Praxis gibt es solche Fälle, bei denen Smart-Home-Geräte entsprechend übernommen wurden, in hoher Zahl. Ein Beispiel ist das sogenannte Mirai Botnetz[19], das bereits für

[19] https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Botnetz_iot_24102016.html

mehrere durchaus wirksame Distributed-Denial-of-Service (DDoS) Angriffe auf große Internetprovider genutzt wurde. Die Übernahme ist jedoch nur eine Möglichkeit. Es können auch Angriffe gegen in Kommunikationsreichweite befindliche Geräte durchgeführt werden oder aber Angriffe gegen die Infrastruktur, in der das Gerät betrieben wird.

Unberechtigter Zugriff und Eingriff

Das zweite Risiko ist der unberechtigte Zugriff und Eingriff in das Produkt und dessen Funktionen. Dadurch wird es möglich, beim Gerät ein ungewolltes bzw. unvorhergesehenes Verhalten zu erzeugen, das für das Gerät selbst und weitere verbundene Geräte zu einem Security- oder potenziell gar Safety-Problem führen könnte. Selbst wenn das Risiko in der Betrachtung für ein einzelnes Produkt als gering einzuschätzen ist, muss in der Risikobewertung auch die Skalierbarkeit berücksichtigt werden.

Fallbeispiel:

Der Hersteller hat ein Gerät, das über eine Möglichkeit zur Laststeuerung verfügt. Gelingt es einem Angreifer, unberechtigten Zugriff auf dieses Gerät zu erlangen, so kann der Angreifer bei einem Einzelgerät nicht viel ausrichten. Ist der Angreifer jedoch in der Lage, dies ausreichend zu skalieren und bedeutet das, eine Vielzahl von Geräten gleichzeitig unberechtigt nutzen zu können, so ist der Angreifer im schlimmsten Fall in der Lage, einen Angriff z. B auf das Energienetz auszuführen.

Verletzung der Privacy

Das dritte Risiko ist die Verletzung der Privacy. Dadurch ist es möglich, dass ein Unberechtigter Zugriff auf vertrauliche und/oder personenbezogene Daten erlangen kann. Dies ist zum einen vor dem Hintergrund der DSGVO (Datenschutz-Grundverordnung) relevant. Zum anderen können die durch unberechtigten Zugriff erlangten Daten anderweitig missbräuchlich genutzt werden. Wird dieser Punkt in der Bedrohungsanalyse identifiziert, muss das Risiko bewertet werden, so dass es gegebenenfalls durch erweiterte Maßnahmen reduziert werden.

Internet of Things (IoT)

Die zunehmende Anzahl der direkt mit dem Internet gekoppelten Endgeräte stellt eine besondere Risikogruppe in einem vernetzten Gebäude dar. Jedes IoT-Gerät stellt ein potenzielles Risiko zur Kompromittierung der IT-Sicherheit dar. Da die meisten Geräte über eine lokale Kommunikationsinfrastruktur auf das Internet zugreifen, besteht das Risiko einer Bedrohung dieser, wenn die Anwendungen auf den Geräten auf das Internet und lokale Ressourcen zugreifen. Hier stellen IP-basierte Endgeräte (Wi-Fi oder Ethernet) das größte Risikopotenzial dar, da sich diese Endgeräte in den meisten Fällen direkt mit Cloud-Plattformen verbinden und somit dem Endverbraucher den Zugriff aus dem Internet erlauben. Diesen Gefahren lässt sich nur begrenzt in der Infrastruktur eines Gebäudes begegnen, sodass diese Geräte einer genauen Betrachtung bedürfen, wenn sie zu einer Dienstleistung im Verbund mit anderen Geräten eingesetzt werden.

7. Basis-Cybersicherheitsmaßnahmen

Wie in Kapitel sechs beschrieben, leiten sich die Schutzmaßnahmen für Cybersicherheit für ein Produkt oder eine Anwendung aus den Risiken ab. Dies ist selbstverständlich immer fallspezifisch, jedoch lassen sich allgemeine Grundsätze beziehungsweise grundlegende Schutzmaßnahmen skizzieren, die in fast allen Fällen sinnvoll anzuwenden sind. Insofern sollen auch keine Security-Funktionen aufgelistet, sondern nur allgemeine Eigenschaften und technologieneutrale Umsetzungsmöglichkeiten genannt werden. An dieser Stelle sei nochmals erwähnt, dass Cybersicherheit nur durch das Zusammenwirken aller Systeme, Komponenten, Akteure und Prozesse wirklich gestärkt werden kann (siehe Vorwort). Konzentriert man sich nur auf Produktfunktionen und den einzelnen Hersteller, dann greift dies zu kurz. Security-by-Design sowie die sichere Installation und der sichere Betrieb der Geräte und Anwendungen müssen Hand in Hand gehen. Wird einer dieser Aspekte im Hinblick auf die Cybersicherheit kompromittiert, gefährdet dies automatisch die gesamte Security-Kette und kann die davorliegenden Maßnahmen unwirksam werden lassen.

„Evergreens“ der Cybersicherheit

Eine Sicherheitsbetrachtung muss von Fall zu Fall erfolgen. An dieser Stelle sollen stichpunktartig Sicherheitsaspekte festgehalten werden, die nach Ansicht der ZVEI-Mitgliedsunternehmen die Cybersicherheit unterstützen und mindestens geprüft werden sollten, ob sie nicht auch für das jeweilige Produkt anzuwenden sind.

Cybersicherheit ist über den gesamten Gebäudelebenszyklus zu berücksichtigen. Dabei liegt es in der geteilten Verantwortung aller beteiligten Parteien den sicheren Betrieb eines Gebäudes zu planen und umzusetzen. Es gilt, bestehende Prozesse und Organisationsstrukturen um die Aspekte der Security zu ergänzen.
Dreh- und Angelpunkt sind hierbei alle beteiligten Personen, die für ihre Tätigkeits- und Verantwortungsbereiche eine entsprechende Sensibilisierung benötigen. Hierzu muss kompetentes Personal in regelmäßigen Trainings zu Leitlinien und Vorgehensweisen unterwiesen werden. Dieses Vorgehen ist entsprechend nachhaltig zu dokumentieren. Dazu gehören unter anderem die vom Betreiber vorgegebenen Leitlinien und Prozessen, z. B. zur Vornahme von Änderungen (Management of Change) und zur Zugriffsberechtigung für Änderungen an Geräten, Arbeitsplatzrechnern und Servern und deren Verbindungen untereinander.

Security-by-Design einer Automatisierungslösung bedeutet, dass Sicherheitsaspekte bereits beginnend mit der Planungsphase zu berücksichtigen sind. Dabei verfolgt die IEC 62443 den systemischen Ansatz, den man in seinen Grundsätzen auch für eine Gebäudeautomatisierung verwenden kann.
Dabei werden folgende Themen für die Implementierung von technischen und organisatorischen Prozessen berücksichtigt, die als Grundlage für die Basisabsicherung einer Gebäudeautomatisierung dienen.

Architektur

Die Sicherheit des Netzwerks fokussiert sich auf alle internen und externen Netzwerkschnittstellen, d. h. Schutz der Kommunikation vor Störungen, Abhören und Manipulation, sowie Schutz des Anlagennetzwerkes vor unbefugten Zugriffen. Eine essenzielle Maßnahme und erster Schritt ist die Segmentierung des Netzwerks. IT- und Gebäudeautomationssysteme sind dabei grundsätzlich zu trennen und die Kommunikation nur soweit wie notwendig zuzulassen. Beispielsweise sollten leistungsrelevante Steuereingriffe (Laststeuerung) nur auf die notwendigen übergeordneten Steuermaßnahmen begrenzt bleiben. Eine weitere Netzsegmentierung ist bedarfsgerecht, z. B. nach der Kritikalität von Betriebsfunktionen, des physischen bzw. logischen Standorts oder als Ergebnis einer Schutzbedarfs- und Risikoanalyse durchzuführen.

Systemhärtung

Unter Systemhärtung versteht man, dass ein System nur die Funktionen zur Verfügung stellt, die zum Betrieb zwingend erforderlich sind. Ziel ist, die potenzielle Angriffsfläche auf ein Minimum zu reduzieren. Durch das Entfernen unnötiger Programme, Dienste, Anwendungen, Konten, Berechtigungen, Ports, Zugriffen usw. haben Angreifer oder auch Malware weniger Möglichkeiten, Anlagen, Systeme, Infrastrukturen, Firmware und Anwendungen zu kompromittieren.

Drahtlose Netzwerke

Bei einem Einsatz von drahtlosen, eigenleitungslosen[20] Übertragungstechniken ist grundsätzlich im Voraus zu klären für welche Anwendung und Zweck der Einsatz

[20] Begriff aus Standard IEC 61131-3; ein anderer Begriff ist z. B. „Powerline“.

erfolgen soll. Ebenso ist eine Schutzbedarfs- und Risikoanalyse für dieses Szenario durchzuführen.

Benutzerverwaltung

Die Benutzerverwaltung berücksichtigt den Zutritt, Zugang und Zugriff zu einem Gebäudeautomationssystem. Hierzu ist ein entsprechender Prozess zu etablieren. Ein wesentliches Prinzip stellt dabei das Minimalprinzip dar, welches sicherstellen muss, dass nur die minimal notwendigen Berechtigungen vergeben werden.

Datensicherung und Wiederherstellung

Die kontinuierliche Verfügbarkeit der Systeme und der von ihnen bereitgestellten Daten ist für den Betrieb von entscheidender Bedeutung. Um potenzielle Systemausfallzeiten und den Verlust oder die Beschädigung/Manipulation von Daten zu minimieren, sollten deshalb entsprechende Strategien zur Sicherung und Wiederherstellung des Gebäudeautomationssystems konzipiert und installiert werden.

Konfiguration und Dokumentation

Die Konfiguration der gesamten Anlage muss erfasst, gesichert und in der Strategie zur Datensicherung und Wiederherstellung berücksichtigt werden. Ebenso sind das gesamte Inventar und alle sicherheitsrelevanten Parameter nachhaltig zu dokumentieren, was bedeutet, dass jegliche Änderungen stets unmittelbar in der Dokumentation aktualisiert werden

Schutz vor Schadsoftware

Für ein wirksames Konzept gegen Malware sind grundsätzlich alle Komponenten des Systems zu berücksichtigen und es müssen angemessene Maßnahmen festgelegt werden. Auf vielen Komponenten der Automatisierungslösung (z. B. SPS, Buskoppler, HMI) kann kein Virenschutzprogramm installiert werden. Durch ausgesuchte Einzelhärtungsmaßnahmen der einzelnen Geräte und das regelmäßige Einspielen von System- und Softwareupdates bzw. -patches kann das Risiko einer Infektion durch Schadsoftware bereits gemindert werden. Alternative Techniken wie Access Control List, Sandboxing, die Kontrolle mobiler Datenträger, Einschränkung von Firmwareupdate, kontinuierliche Überwachung und Einbeziehung von Überwachungswerkzeugen im Automatisierungssystem sind hier mit einzubeziehen.

Fernzugriff

Bei Fernzugriffen müssen die Integrität und Vertraulichkeit der Daten sowie die Authentifizierung der Kommunikationspartner sichergestellt werden. Als etablierter Schutzmechanismus haben sich verschlüsselte Verbindungen bewährt. Insbesondere für den Fernzugriff bzw. die Fernwartung sind dies verschlüsselte VPN-Verbindungen (z. B. über IPsec/Internet Protocol Security), die den Schutz von Integrität, Vertraulichkeit und Authentizität sicherstellen.

Patch Management

Die organisatorischen Maßnahmen sollten einen Prozess zum Änderungsmanagement im Betrieb der Gebäudeautomation enthalten. Beim Patchmanagement-Prozess ist grundsätzlich zwischen Patch, Updates und Upgrades zu differenzieren. Während ein Patch nur Fehlerkorrekturen durchführt, können bei einem Update auch neue Funktionalitäten enthalten sein. Dadurch besteht nach der Installation von Updates ein höheres Risiko unerwünschter Nebeneffekte durch Veränderungen. Bei jedem Patch- oder Update-Prozess ist zu berücksichtigen, inwieweit die ursprünglich zugesicherte (systemweite) Funktionalität weiterhin vollumfänglich und uneingeschränkt gewährleistet wird. Daher sollte das Ausrollen bewertet und kontrolliert erfolgen, d. h. auch immer unter Einbeziehung der verantwortlichen Personen. Sofern die Möglichkeit besteht, sollten Änderungen in einer Testumgebung verifiziert werden[21].

Steuerung von Ereignissen

Im Allgemeinen sollte definiert werden, was für die Anlage als sicherheitsrelevantes Ereignis verstanden wird und es sollte ein Prozess mit beschriebenen Abläufen und Verantwortungen geschaffen werden. Darin muss beschrieben werden, wie bei Auftreten eines Ereignisses zu verfahren ist und welche Rollen (ggf. Personen) agieren müssen.

[21] Der ZVEI vertritt zum Thema Patch Management noch keine einheitliche Position, daher gibt dieser Absatz lediglich die Einschätzung der Task Force Cybersicherheit im Gebäude wieder.

8. Fazit

Stetige Veränderungen bestimmen unsere Lebens- und Arbeitswelt im Allgemeinen und im Hinblick auf Cybersicherheit im Besonderen. So haben sowohl gesellschaftliche Veränderungen als auch technologische Entwicklungen und sogar biologische Gefahren, wie eine weltweite Pandemie, Auswirkungen auf dieses Phänomen. Der Begriff, des „Moving Targets“ der Cybersicherheit ist inzwischen weithin bekannt, hat aber nichts an seiner Aktualität verloren. Vielmehr haben uns die Entwicklungen vor allem in den vergangenen zwei Jahren gezeigt, welche Herausforderungen existieren und dass diese beherzt angegangen werden müssen. Die Bedeutung des Homeoffices hat schlagartig zugenommen und wird voraussichtlich weiterhin auf hohem Niveau verbleiben. Der gesamten Gesellschaft und Wirtschaft wurde transparent vor Augen geführt, dass es kein Zurück in der Frage der Digitalisierung und Vernetzung geben sollte und geben wird. Besonders nicht, wenn Deutschland seine Position als innovativer Wirtschaftsstandort weiterhin verteidigen und ausbauen möchte. Ein angemessenes Niveau der Cybersicherheit ist dabei aber eine notwendige Voraussetzung, um die Potenziale einer digitalisierten und vernetzten Welt heben zu können. Nur mit ihr können neue Formen der Problemlösung, digitale Geschäftsmodelle sowie sektorübergreifende Dienstleistungen und Zusammenarbeit erfolgreich realisiert werden.

Denn nur mit Innovationen sowie einer umfassenden Elektrifizierung und Digitalisierung lassen sich die Herausforderungen, die sich an unsere Gesellschaft stellen, lösen und die bevorstehenden Veränderungen meistern. Das vernetzte Gebäude bietet dabei sowohl Lösungsansätze, welche die demographische Entwicklung der Gesellschaft abfedern, als auch die Chance, mit mehr Energieeffizienz und weniger CO_2-Ausstoß im Gebäudesektor einen wichtigen Betrag zum Klimaschutz zu leisten.

- Diese Funktion der Cybersicherheit als Vorbedingung der Digitalisierung bringt dabei eigene Herausforderungen mit sich.

- Cybersicherheit kennt keine Ländergrenzen und die technische Entwicklung wird und sollte weltweit vorangetrieben werden. Internationale Standardisierung ist für die Interoperabilität und nachhaltige, unternehmerische Aktivitäten daher unerlässlich.

- Mit voranschreitender Vernetzung verschwimmen die Domänengrenzen und klare Abgrenzungen werden zunehmend schwerer. Die Adressierung der erforderlichen Anforderungen muss also in geteilter Verantwortlichkeit erfolgen, sodass alle Beteiligten ihren Beitrag leisten, um das System zu sichern.

Die stetige Weiterentwicklung sowohl hinsichtlich der Bedrohungslage als auch ihrer technischen und organisatorischen Entgegnung sowie die allgemein voranschreitende technologische Entwicklung erfordern eine kontinuierliche Bewertung des Themas. So ist zu erwarten, dass auch dieser deutlich erweiterte Stand des Whitepapers „Basis-Cybersicherheit in vernetzten Gebäuden“ nur einen Augenblick festhält und es einer weiteren stetigen Anpassung bedarf.

Anhang 1: Orientierungshilfen für weitere Recherchen

Umsetzungshilfen:

Orientierung IoT Security: ENISA Baseline Security Recommendations for IoT

Basis-Cybersicherheit vernetzbares (Industrie-)Gerät: BSI Anforderungen an netzwerkfähige Industriekomponenten

Produktentwicklung und Produkt-Security: IEC 62443 Teil 4-1 und 4-2

Bilden von Security-Level für Produkte und Organisation: IEC 62443 Teil 3-3

Sichere Identitäten: Whitepaper Sichere Identitäten (Plattform Industrie 4.0)

Basis-Absicherung: BSI Leitfaden zur Basis-Absicherung nach IT-Grundschutz

Managementsystem: ISO 27001

Managementsystem für softwaregesteuerte Komponenten: VdS 3836

Domänenübergreifende Adressierung: VDE-Anwendungsregel DE-AR-E 2802-20

Für Risikoanalyse/Bedrohungslagen:

ENISA: Threat Landscape

BSI: Cyber-Sicherheitslage

In Kraft befindliche Gesetze:

BSI-Gesetz, geändert durch IT-Sicherheitsgesetz 1 & 2

Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie)

EU Cybersecurity Act

Delegierter Rechtsakt unter Art. 3(3) d/e/f der Funkanlagenrichtlinie (Radio Equipment Directive, RED) (Datum der Anwendbarkeit: 01.08.2024)

In Vorbereitung befindliche Gesetzesvorhaben:

Review der Richtlinie zur Netz- und Informationssicherheit (NIS-2-Richtlinie)

Cyber Resiliance Act (CRA)/horizontale Produktregulierung

Übersichten und Positionspapiere

- ZVEI-Stellungnahme zum Referentenentwurf des IT-Sicherheitsgesetz 2.0:

  IT-Sicherheitsgesetz 2.0 - Stellungnahme zum aktuellen Referentenentwurf (zvei.org)

- Stellungnahme zum Entwurf einer Rechtsverordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik: https://www.zvei.org/themen/cybersicherheit?showPage=3208811&cHash=40f6944211f2832ea6b571854ece8975

- ZVEI- Whitepaper Horizontale Produktregulierung für Cybersicherheit:

  Horizontale Produktregulierung für Cybersicherheit (Whitepaper) (zvei.org)

- BDI-DIN/DKE-Positionspapier für eine europaweite horizontale Cyberregulierung:

  Europaweite Cyberregulierung (bdi.eu)

- Orgalim Positionspapier für eine horizontale Produktregulierung für Cybersicherheit im NLF:

  Digital Transformation: Proposal for a horizontal legislation on cybersecurity for networkable products within the New Legislative Framework | Orgalim

- ZVEI-Diskussionspapier: Horizontale Prozessanforderungen für das Security Life-Cycle Management von IoT-Produkten

Anhang 2: Erläuterungen wichtiger Grundbegriffe

Identifikation: Unter Identifikation versteht man einen Vorgang, der zum eindeutigen Erkennen eines Geräts/ Objekts dient. Ein Kommunikationsteilnehmer sagt dem anderen, wer er ist.
Authentifizierung: Unter Authentifizierung versteht man einen Vorgang, der eindeutig beweist, dass der richtige Kommunikationspartner adressiert ist. Ein angesprochener Kommunikationspartner legt dem anfragenden Gerät den Beweis vor, dass er wirklich berechtigt ist, mit ihm Informationen auszutauschen.

Identifizierung und Authentifizierung stellen sicher, dass die informationsaustauschenden Geräte die richtigen Partner sind und dass sie auch berechtigt sind, Informationen untereinander auszutauschen.

Rollen und Rechtemanagement legt fest, wer in einem System welche Zulassung zu bestimmten Funktionen zugewiesen hat. Eine **Rolle** beinhaltet eine Sammlung von Rechten und weiterer Spezifikationen, die einem oder mehreren Anwendern zugeteilt werden können. Es sind in einem System Rollen zu definieren und dann diesen Rollen entsprechende Eigenschaften im Sinne von Rechten zuzuweisen. Typische Rollen sind z.B. Benutzer, Inbetriebsetzer, Wartung oder auch Administrator.

ZVEI: Der Verband der Elektro- und Digitalindustrie

Der ZVEI vertritt die gemeinsamen Interessen der Elektro- und Digitalindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland und auf internationaler Ebene.

Die Branche beschäftigt rund 877.000 Arbeitnehmer im Inland. 2021 lag ihr Umsatz bei rund 200 Milliarden Euro.

Fast ein Viertel aller privaten F+E-Aufwendungen in Deutschland kommen von der Elektroindustrie. Jährlich wendet die Branche rund 20 Milliarden Euro für F+E auf und mehr als sechs Milliarden Euro für Investitionen. Ein Drittel des Branchenumsatzes entfallen auf Produktneuheiten. Jede dritte Neuerung im Verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der Elektroindustrie.

Basis-Cybersicherheit in vernetzten Gebäuden

Version 2.0

Herausgeber:
ZVEI e. V.
Lyoner Str. 9
60528 Frankfurt am Main

Verantwortlich:
Sanaz Khedri
Telefon: +49 69 6302-222
E-Mail: sanaz.khedri@zvei.org

www.zvei.org

Februar 2022