Whitepaper

Basis-Cybersicherheit in vernetzten Gebäuden

Handlungsoptionen und Orientierungshilfen

Version 1.2, Juni 2020*

Zentralverband Elektrotechnik- und Elektronikindustrie

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

Inhalt

Vorwort 3

1 Scope: Vernetztes Gebäude 4

2 Vernetzung und Digitalisierung im Gebäude 5

3 Generisches Architekturbild 6

4 Risikoanalyse 7

Betrachtungsgegenstand der Risikoanalyse 7

Aufbau einer Risikoanalyse 7

Methoden für die Risikoanalyse (Beispiel) 9

Verankerung der Risikoanalyse in der Organisation 9

5 Grundlegende Risiken für das vernetzbare Gebäude 10

Modifizierung der Anwendungssoftware 10

Unberechtigter Zugriff und Eingriff 10

Verletzung der Privacy 11

6 Basis-Cybersicherheitsmaßnahmen 12

Anhang 1: Orientierungshilfen für weitere Recherchen 13

Anhang 2: Erläuterungen wichtiger Grundbegriffe 13

Vorwort

Vernetzung und Digitalisierung sind ohne Cybersicherheit (hier engl. Security) 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- und Servicequalität wird. Vor diesem Hintergrund besteht Handlungsbedarf. Die ZVEI-Mitglieder skizzieren mit dem vorliegenden Whitepaper Überlegungen zur Weiterentwicklung des Stands der Technik. Dies ist wichtig und dringlich, denn Cybersicherheit ist eine zentrale Grundlage für das Kundenvertrauen und damit der Geschäftsprozesse und für die Gesellschaft insgesamt. Das Whitepaper steht vor diesem Hintergrund für das klare Commitment der ZVEI-Mitgliedsunternehmen, den bereits begonnen Weg entschlossen fortzuführen. Viele Maßnahmen wurden bereits in den Produkten und Anwendungen umgesetzt. Doch soll die Cybersicherheit kontinuierlich weiterentwickelt werden. Die Weiterentwicklung der Cybersicherheit 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 und Systemen werden;
2. muss angesichts der dynamischen Entwicklung des Risikoumfeldes (Cybersicherheit als „Moving Target“) flexibel und stets risikobasiert gestaltet werden;
3. umfasst den gesamten Lebenszyklus eines Produktes, das heißt die Entwicklung, Fertigung, Inbetriebnahme, den Betrieb und die Außerbetriebnahme eines Produktes 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 möglich werden.

1 Scope: Vernetztes Gebäude

Das Whitepaper untergliedert „vernetztes Gebäude“ nicht weiter in Wohn- und Zweckbauten 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.[1] 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 Zweckbau 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, auch wenn in unterschiedlicher Ausprägung:

- Heizung, Lüftung, Wasser und Klimatisierung
- Beleuchtung und Elektroinstallation
- Energiesysteme und -steuerung
- Komfort und Entertainment
- Sicherheitstechnik

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

[1] https://www.dke.de/resource/blob/778214/6ec4d037024b61a63d14544d181c638a/deutsche-normungs-roadmap-smart-home---building--version-2-0-data.pdf

2 Vernetzung und Digitalisierung im Gebäude

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. Zusätzliche 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 mittelbare oder direkte Verbindung mit dem Internet ein entscheidender Parameter für die Einschätzung. Vor diesem Hintergrund erscheint eine grobe Unterscheidung zwischen einer

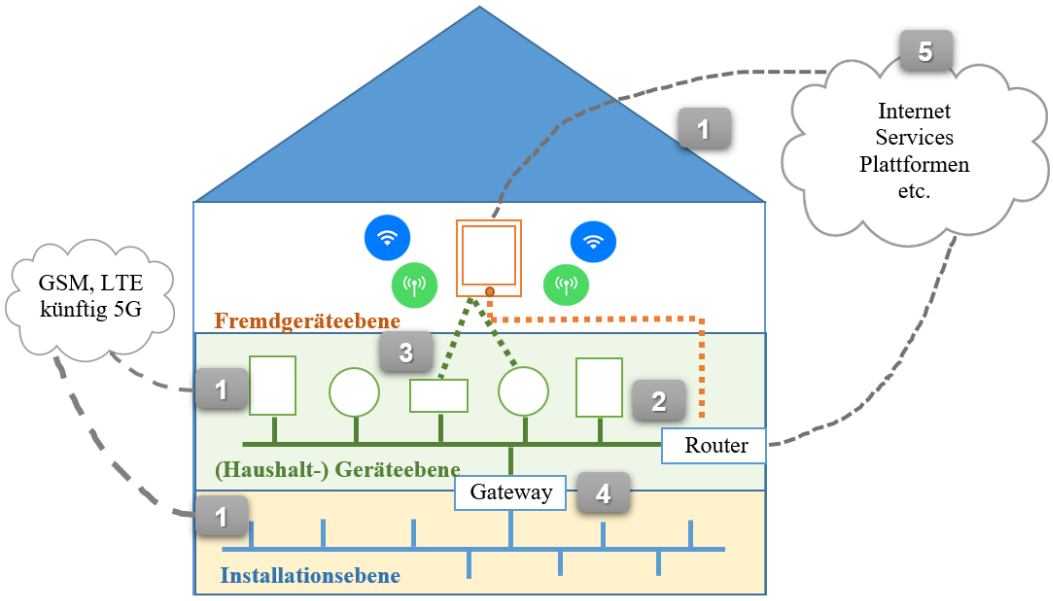
- rein lokalen (siehe Installationssysteme),
- Punkt-zu-Punkt (siehe weiße und braune Ware) und
- direkter Internet-Vernetzung (siehe Kommunikationsgeräte wie Handys und Tablets) sinnvoll.

Digitalisierung und Vernetzung zusammen wirken sich 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 werden. 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 die Cybersicherheit im Gebäude entsteht.

3 Generisches Architekturbild

Grundsätzlich hat die 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 4).

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.



Anhand des Architekturbildes lassen sich mindestens fünf zentrale Punkte feststellen, die im Hinblick auf die Cybersicherheit adressiert werden müssen. Selbstverständlich ist 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 zum Internet und Mobilfunk, sprich zum Beispiel Geräte, die über einen eigenen Netzzugang oder Funkmodul verfügen.
2. Router als zentrale „Gateways“ zu den Geräten und Systemen im Gebäude.
3. Die Punkt-zu-Punkt-Verbindung von Haushaltsgeräten mit Handys, Tablets etc., wodurch eine indirekte Verbindung mit dem Internet und Mobilfunk entsteht.
4. Gateways und sonstige Übergänge zur Gebäudeinfrastruktur und fest verbauten Installationssystemen.
5. Über das Internet angebundene Backendsysteme.

4 Risikoanalyse

Cybersicherheit kann sinnvoll nur im Hinblick auf die vorgesehene Verwendung der Geräte und Anwendungen und den damit einhergehenden relevanten Risiken gestaltet werden. Andernfalls laufen Maßnahmen ins Leere und verschwenden Geld, Zeit und 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.

Betrachtungsgegenstand der Risikoanalyse

Eine Risikoanalyse kann methodisch auf verschiedene Art und Weise vorgenommen werden. Das Whitepaper spricht sich bewusst nicht für eine bestimmte Methodik aus. Wichtiger ist, dass die relevanten Aspekte einer Risikoanalyse klar sind: Was ist und was ist nicht in einer Risikoanalyse zu bewerten? Folgende Punkte sind lediglich wichtige Schlüsselelemente einer Risikoanalyse, jedoch definitiv nicht eine abschließende Auflistung:

- der Einsatzort und Einsatzzweck des Gerätes, des Systems oder der Anwendung
- die 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
- die Netzwerk-, Protokoll- und Kommunikationsschnittstellen und damit die Art der Vernetzung mit dem Internet und Mobilfunknetz (direkt, indirekt, getrennt etc.)
- eventuelle Backend-Systeme und Services
- die Abgrenzung zu anderen Systemen und Aspekten, die nicht beeinflusst werden können

Aufbau einer Risikoanalyse

Zu Beginn einer Risikoanalyse sind die relevanten Unternehmenswerte und -prozesse zu identifizieren und hierfür der Schutzbedarf 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“).

Beispielhafte Ergebnistabelle

#	Gegenstand	Risikoklasse	Begründung / Herleitung	Schutz-maßnahme
1	Gerät X	mittleres Risiko	Auf dem Gerät kann Software von Drittanbietern ausgeführt werden	a, b, c ... mit Prio 1, 2 und 3
2	Gerät Y	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
3	Gerät Z	hohes Risiko	Gerät ist über IP-vernetzt und kann Software aktiv ausführen	a, b, c ... mit Prio 1, 2 und 3

Das Ergebnis ist dann die Grundlage für die Auswahl der zu implementierenden Sicherheitsmaßnahmen und deren Skalierung. Die Maßnahmen leiten sich hierbei von dem jeweiligen Risiko ab. Für die konkrete Auswahl der Maßnahmen geben die ISO 27002 oder die Maßnahmenkataloge des BSI IT-Grundschutzes[2] Hilfestellungen. Dieses Vorgehen sorgt für Effizienz und Investitionssicherheit und erleichtert die Serienpflege der Produkte. Des Weiteren ermöglicht dies die Erfüllung weiterer regulatorischer Vorgaben, wie beispielsweise die Produktbeobachtungspflicht im Zuge der Marktüberwachung.

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.

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

Methoden für die Risikoanalyse (Beispiel)

Für die Durchführung der Risikoanalyse gibt es standardisierte Vorgehensmodelle. Allgemein sollte anhand der Schutzziele Vertraulichkeit (Confidentiality), Integrität (Integrity) und Verfügbarkeit (Availability) – der sogenannten CIA-Triad – für das jeweilige Produkt oder die Anwendung immer eine Bewertung der Risiken erfolgen. Standardisierte Vorgehensmodelle wie beispielsweise STRIDE[3] 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**.

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 werden sich in vielen Unternehmen spezialisierte Rollen für Product and Solution Security etablieren. Ein Team von Produkt-Cybersicherheitsexperten kann zu einem sogenannten Product Computer Emergency Response Team (P-CERT) zusammengefasst werden, das gegebenenfalls für einzelne oder alle Produktgruppen dauerhaft Risikoanalysen durchführt, die Ergebnisse verarbeitet und für akute Vorfälle bereitsteht.

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

5 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. die Destabilisierung des Energienetzes durch manipulierte Geräte
3. die 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

Modifizierung der Anwendungssoftware

Das erste Risiko ist die unberechtigte Modifizierung der Anwendungssoftware eines Produktes. Das Risiko besteht darin, dass die Software eines Produktes 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. 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[4], welches bereits für 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 ist es möglich, beim Gerät ein ungewolltes beziehungsweise unvorhergesehenes Verhalten zu erzeugen, das für das Gerät selbst und weitere verbundene Geräte zu einem Security- oder Safety-Problem führen kann. Selbst wenn

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

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 nun 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 nutzten 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, so muss das Risiko bewertet werden, so dass dieses gegebenenfalls durch erweiterte Maßnahmen reduziert werden.

6 Basis-Cybersicherheitsmaßnahmen

Wie in dem vorherigen Kapitel beschrieben, leiten sich aus den Risiken die Schutzmaßnahmen für Cybersicherheit für ein Produkt oder eine Anwendung ab. Dies ist selbstverständlich immer fallspezifisch, d. h. eine Security-Betrachtung muss von Fall zu Fall beziehungsweise von Produkt zu Produkt erfolgen. Es lassen sich jedoch in fast allen Fällen allgemeine Grundsätze beziehungsweise grundlegende Schutzmaßnahmen der Cybersicherheit (allgemeine Eigenschaften und technologieneutrale Umsetzungsmöglichkeiten) sinnvoll anwenden. An dieser Stelle sei nochmals erwähnt, dass Cybersicherheit nur durch das Zusammenwirken aller Elemente, 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, dann gefährdet dies automatisch die gesamte Security-Kette und kann die davorliegenden Maßnahmen unwirksam werden lassen. Hier können entsprechende Standards helfen sowohl funktionale Sicherheitsanforderungen als auch Anforderungen an Prozesse zu erfüllen.[5]

[5] Welche Anforderungen an Prozesse sich dabei mindestens in zukünftigen (sektoralen) Normen widerfinden sollten hat eine übergreifende ZVEI-Arbeitsgruppe erarbeitet. Ihre Empfehlungen für Prozessanforderungen sind hier zu finden: https://www.zvei.org/presse-medien/publikationen/horizontale-prozessanforderungen-fuer-das-security-life-cycle-management-von-iot-produkten/

Anhang 1: Orientierungshilfen für weitere Recherchen

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

Anhang 2: Erläuterungen wichtiger Grundbegriffe

Identifikation: Unter Identifikation versteht man einen Vorgang, der zum eindeutigen Erkennen eines Gerätes/ Objektes 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.

Basis-Cybersicherheit in vernetzten Gebäuden (Version 1.2)

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.

Lyoner Str. 9
60528 Frankfurt am Main

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

www.zvei.org

Juni 2020