ZVEI: Die Elektroindustrie

White Paper

Basic cybersecurity in networked buildings

Courses of action and orientation aids

Version 2.0 – Status as at February 2022*
Germany's Electro and Digital Industry Association

* Cybersecurity is a rapidly evolving topic.
The positioning of ZVEI is therefore continuously adjusted.

Contents

Foreword

The COVID-19 pandemic has caused massive changes in many areas and significantly impacted our lives, our homes and our workplaces. One of the main work-related process changes, especially in terms of the scope of use, is the enormous increase in the importance of remote work. With a view to global CO_2 reduction targets, this trend is expected to persist beyond the current crisis. The shift of work activities to employees' homes, however, has also brought a shift in cyberattacks and a renewed focus on the home as a target. It can be assumed that companies will face a wave of malware coming from home offices.[1]

Digitisation in the Smart Home sector and increasing networking in the Smart Building field are a significant driver. The home is indisputably the setting with the highest IoT penetration. This is evidenced in the digitisation index as well as numbers on IoT usage[2]. This trend will only intensify, especially given that intelligent building automation is the only way to harness the enormous sustainability potential for increased efficiency and the associated reduction of CO_2 emissions from buildings.[3]

Social and demographic changes (age pyramid), such as the increasing number of people requiring care who want to remain in their own home, are also making Smart Home applications even more important.

The German market is unusual in that it has a low home ownership rate of approximately 51 percent but also a high share of single-family homes (around 16 million) [4]. It can therefore be characterised as a tenants' market.

Germany has a high ratio of non-residential buildings with technical amenities. This results in a high degree of networking and the formation of a corresponding service landscape.

These aspects must be considered when evaluating the information security of a building and its systems. The large, heterogeneous group of stakeholders makes addressing the respective areas of responsibility a particular challenge. Coordination

[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

is therefore crucial when allocating the various functions to ensure an adequate level of IT security.

ZVEI is addressing these challenges by bundling these topics in its Buildings platform and, in particular, in its task force on cybersecurity in buildings. Firstly, this white paper is intended to provide building owners and operators with an orientation aid in this complex and dynamic environment. Secondly, it is meant to help the responsible employees within companies (product management, process development, research and development, and corporate management) consider the topic of cybersecurity early in the decision-making process for new products.

1. Cybersecurity in buildings: “Challenges and shared responsibilities”

Networking and digitisation cannot advance without cybersecurity in products and applications. This is a core principle for the manufacturing companies organised within ZVEI. They moreover aim to make cybersecurity an integral component of product, system and service quality. There is a need for action in this area. In this white paper, the members of ZVEI outline considerations regarding future developments, the current state of the art, processes and organisational structures. This is important and urgent, as cybersecurity is a central foundation of customer trust, functioning business processes and our increasingly digitised society as a whole. In this context, the white paper highlights the commitment of ZVEI’s member companies to resolutely continue down their stated path. Many measures have already been implemented in products and applications, but cybersecurity must be continuously strengthened. However, this further development can only succeed as an overarching responsibility shared by all stakeholders. Additional basic principles that must be considered:

Cybersecurity...

1. will become an integral component of networked products, systems and services;
2. must be designed flexibly and always take risks into account due to the dynamic development of the risk environment (cybersecurity as a moving target);
3. encompasses the entire life cycle of a product – including the development, production, commissioning, operation and decommissioning of a product – and cannot be reduced to Security by Design;
4. must accordingly be approached as a responsibility distributed across the product life cycle and consistently shared by manufacturers, integrators, installers, operators and users.

The European and international export markets furthermore form the natural reference framework for the further development of cybersecurity. Isolated national strategies are not a viable alternative, and they can jeopardise the competitiveness of companies. Rather, an international dialogue is needed to reinforce compatibility, interoperability and innovative potential. Together, the members of ZVEI will rise to meet the challenges of cybersecurity. To do so, they rely on European approaches as envisioned in the EU Cybersecurity Act, the Delegated Act on Article 3 (3) d/e/f of the Radio

Equipment Directive, and especially through horizontal product regulation as laid out in the European product safety law, the New Legislative Framework (NLF). Europe must address this issue consistently and make the requirements coherent, efficient and effective in their implementation. International connectivity should not be neglected, though, particularly since other world regions like China and the US are also working intensively on appropriate mechanisms.

- The following challenges must be addressed here: Especially in rented infrastructure, the interplay between Smart Home products (newly installed by tenants, for example) and the existing building infrastructure represents a challenge in terms of cybersecurity. Interfaces become even more crucial with the use of such products via “joint operations” in “semi-public infrastructure”.

- Landlords and investors often find themselves in an investment dilemma: On the one hand, the return on investment is not always clear for digitisation measures, especially for residential buildings. On the other hand, investments in digitisation of non-residential buildings can serve to substantiate a quality level in terms of convenience, security and economic efficiency, thereby increasing rentability. The political discussions should increase investors’ ability to plan.

- Smart Home products will take on an increasingly important support role for an ageing society with more people requiring care. This includes both assistance that could be provided when a need for care is determined in accordance with German health regulations, and the entire field of ambient assisted living, which enables the implementation of Smart Health solutions, lifelong residential design and other innovative concepts that improve quality of life.

- The aforementioned advance of digitisation causes an increase in cybersecurity challenges; the danger of compromised IT systems rises with IP penetration.

- As implementation of a cloud-based service landscape forges ahead, further requirements and consequences will arise.

- The challenges of shared responsibility must be taken into account when defining the various roles and by the people who fill those roles. No one will presumably be able to offer all the products required to set up a complete Smart Home environment; rather, products from various manufacturers will have to be considered and integrated. At the same time, there are barely any stakeholders in the Smart Home field who have a complete view of the system in terms of its connections to the “outside”.

- This challenge will only grow larger in the future thanks to new players who enter the Smart Home market with their own business models, ecosystems and security architectures, thereby setting de facto standards while not necessarily prioritising interoperability with the rest of the Smart Home environment.

2. Application area: Networked building in the midst of digitisation

This white paper consciously does not consider critical infrastructures.[5] Addressing the digitisation of networked buildings and the associated products and solutions, which are sold globally, requires at least a European-level approach. After all, these products and solutions are available globally but must nevertheless be implemented as required by the respective regions, especially when they play a pioneering role. In turn, though, national requirements in Germany as a leading market – particularly at the interface of buildings and the energy system – must be taken into account and, ideally, aligned with European standards.

This white paper does not break down the category of networked buildings further into residential and non-residential buildings, i.e. “Smart Home” and “Smart Building”. For passages that do reference the Home and Building categories, the paper understands the terms as defined in the DKE Smart Home + Building Standardisation Roadmap.[6] The term “networked” or “networkable buildings” is used here as a collective term for both building types.

Considering cybersecurity jointly for both building types simplifies our assessment. Although the responsibilities, competencies and legal basis are different for residential and non-residential buildings, there are still common starting points and considerations with regard to cybersecurity. In simple terms, the white paper assumes that devices connected to the Internet both directly and indirectly may be installed in a networked building. Another assumption is that all networked buildings will feature the following components to varying degrees:

- Heating, ventilation, water and air conditioning
- Lighting and electrical installation
- Energy systems and control
- Modern conveniences and entertainment
- Security technology and technical surveillance sensor systems
- Small office/home office (SOHO)
- Household appliances[7]

[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
[7] Household appliances are only considered in the context of their respective connection to the building infrastructure/IT systems.

The affected trades should assess cybersecurity both individually and collectively as a system. The combined evaluation of residential and non-residential buildings has no negative impact for the level of basic cybersecurity, which is to be the exclusive focus of this white paper.

3. Networking and digitisation in Home & Building

Networking and digitisation take place at several levels in networked buildings. In the Smart Home and Smart Building contexts, however, these terms are often bundled in a confusing way. This white paper is based on the following differentiation:

Digitisation: Analogue data is digitised. In addition, analogue and/or digitised data is made useful via provision, processing, visualisation and storage.

Networking: Previously unconnected objects and data (digital and analogue) are connected to each other.

There can be varying degrees of networking. In terms of cybersecurity, the points of access and therefore the indirect or direct connection to the Internet are a crucial parameter for the evaluation. It makes sense here to roughly differentiate between

- the purely local exchange of information (e.g. installation systems),
- local information structures connected to the Internet
    - e.g. point-to-point (white or brown goods) and
- direct Internet networking (e.g. IoT devices or communication devices such as mobile phones and tablets).

Communication devices and systems based on open communications media (e.g. WiFi, radio frequency, other radio networks, power-line) must be considered according to their characteristics. This publicly accessible transmission of information requires a corresponding appraisal at the communication level and can also be compensated at the data and/or application level.

Digitisation and networking have a direct impact on the cybersecurity of networked buildings and the products they contain. The potential points of attack are multiplying, and attacks can scale up far more quickly in such buildings and across the entire Internet of Things, meaning that many more devices and systems can be affected by cyberattacks in a very short amount of time. Cyberattacks are no longer limited to single domains, since domain boundaries have been progressively blurred by networking. It is therefore all the more important to define comprehensive, foundational requirements and measures for cybersecurity. This ensures that every product, system and trade can

make its capability and risk-based contribution to the overarching cybersecurity of the building.

Advancing digitisation and data processing will increasingly give rise to applications that go beyond the simple networking of devices. The security review must therefore involve the sophisticated implementation of necessary security measures in a multi-step process (regarding product integration) as required for the applications and services from both a regulatory and consumer view.

It would be neither practical nor expedient to apply the overall requirements to all devices and systems involved in the delivery of services. The necessary system security in a networked home and building must be evaluated in a multi-step risk analysis for the relevant components. This a precondition for taking suitable measures.

Changes during the life cycle[8] of the overall system must be taken into account with a new risk assessment for each new threat situation.

[8] The service life of buildings is not directly comparable with that of consumer goods, since buildings are typically used much longer. Furthermore, infrastructures have different service lives than the services that use them.

4. Generic architecture model: Overall view of application areas

The fundamental task of cybersecurity is to protect the confidentiality, integrity and availability of information, things and data in the face of numerous threats. These three security goals are the foundation of every security consideration. This white paper outlines three threats that significantly influence the cybersecurity of networked buildings: the modification of application software, unauthorised access to products and violations of privacy (see Chapter 5).

The starting point for our consideration of cybersecurity and these threats is a generic architecture model of a networked building. An architecture model like this can clearly be configured any number of different ways and implemented differently in reality.

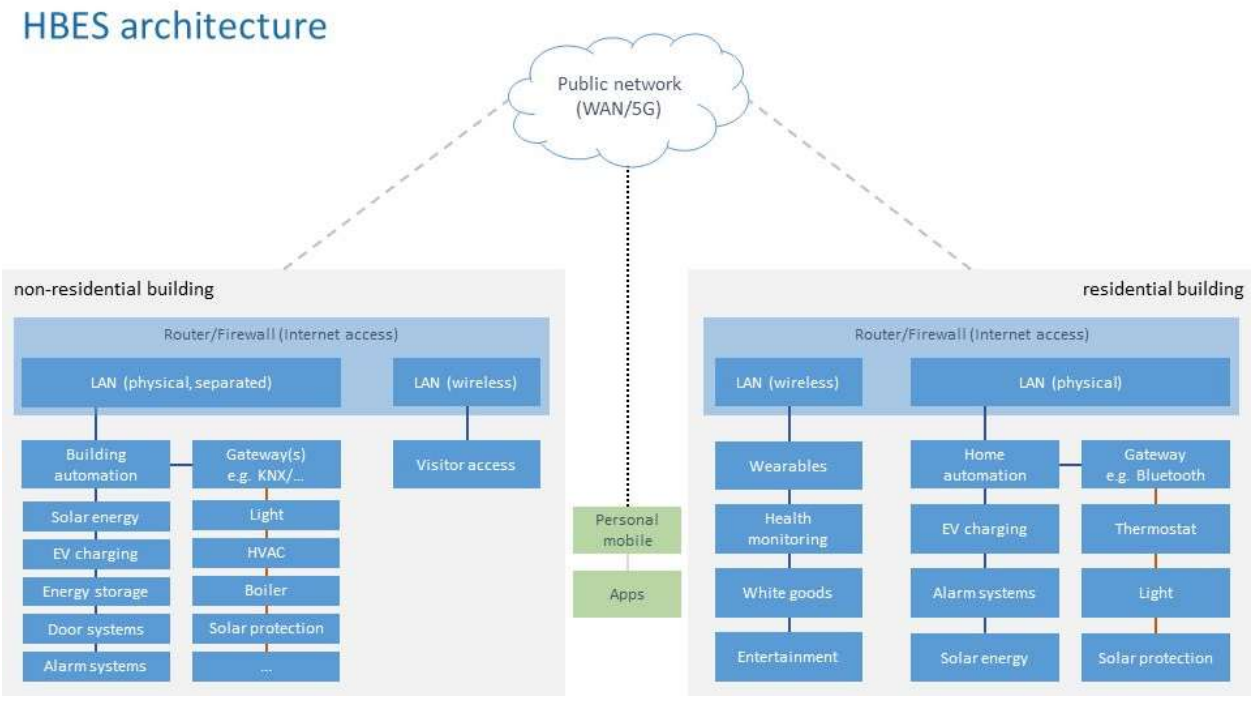

Figure 1: Architecture variants (simplified) for an IT connection of a home and building electronic system (HBES)[9]

With a view to the different IT connection options (architecture variants), we can determine at least five central points that need to be addressed in relation to cybersecurity. Of course, this list is not to be seen as exhaustive or comprehensive. It is meant to provide an initial orientation but cannot replace a dedicated security review:

[9] Non-residential building: As noted in Chapter 2, critical infrastructure buildings, which may be subject to special requirements, are excluded here.

1) The devices with a direct connection to the Internet and mobile network, such as devices with their own network access or wireless module.
2) Routers as central gateways to the devices and systems in the building.
3) The point-to-point connection of household appliances to mobile phones, tablets etc., which creates an indirect connection to the Internet and mobile network.
4) Gateways and other interfaces to the building infrastructure and permanently installed systems.
5) Backend systems connected via the Internet.

The various architecture variants shown in Figure 1 differ widely in their technical implementation in terms of data, applications and communication protocols. To enable a differentiation here, it helps to delimit the information layer from the application layer and the communication layer. The Home and Building Architecture Model Framework groups the relevant components and divides the technical aspects into zones according to their data integration.

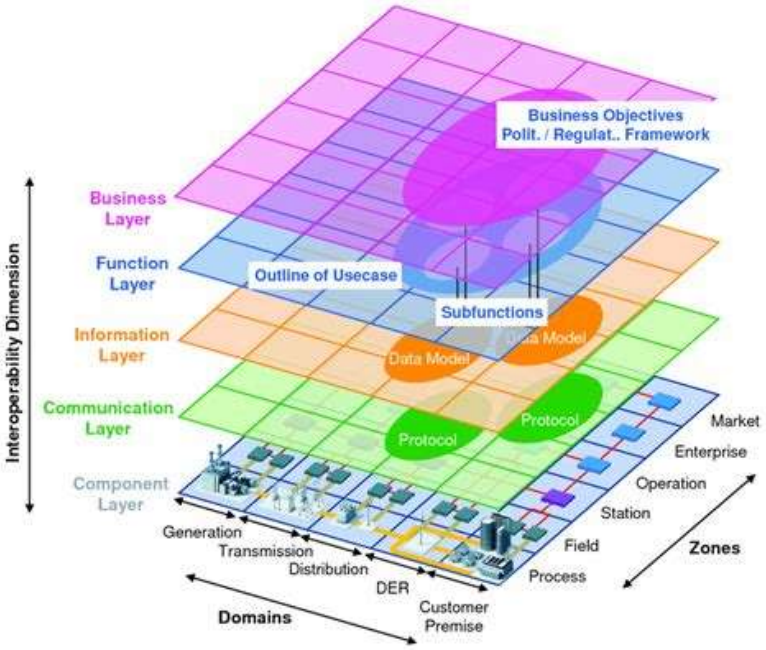

Figure 2 Home and Building Model Framework[10]

The Home and Building Model Framework (Figure 2) describes the topic areas assigned to end consumers from a standardisation perspective. End consumers are the focus of this model framework, and the ecosystem is built around them. Rather than setting stipulations for IT architectures, it describes and models the complexities within

[10] The image was created based on the reference architecture for Industry 4.0. 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

homes and buildings. It also draws connections between the different topic areas and components.

Especially with a view to the differentiated implementation of security measures, it is possible to model interoperable systems that are technically capable of interacting but still allow for scaling in terms of data access and usage. This nuanced approach is necessary to avoid the static implementation of cybersecurity measures and enable a flexible, application-oriented implementation.

Technology trends:

- IP-based network structure is becoming dominant. The jointly used IP infrastructure enables links between systems from different domains and even cloud functions. Configuration, operation and maintenance take place on IP-based systems.
- The IP infrastructure is on a halfway point on the path to cross-application continuity; the crucial precondition for simple links is semantic interoperability – semantic interworking – at the application layer. Semantic interworking refers to integration via the use of common information modelling or ontologies and thus the coexistence of technologies as well as a common representation of technology with mapping that can be configured and expanded on an abstracted level.
- The integration of digital twins into a digitised building infrastructure (Building Information Modelling – BIM)

Functional trends:

- The trend is towards higher connectivity and “always on” Internet access; connectivity is a key requirement for practically all building applications.
- The scope of building functionality and the required technical equipment is growing in both residential and non-residential buildings. This is leading to a high concentration of technical applications. All functions are linked to one another.
- Buildings are becoming prosumers in the power grid or even entirely self-sufficient in terms of their energy provision.
- The diversity and scope of service connections is growing.

Social trends:

- In 2020, around 37 percent of residents in Germany's 19.2[11] million residential buildings used at least one Smart Home application, and the figure was 50 percent for those over 50.
    - The focus is on three main areas: a) energy &climate, b) security and c) home & garden.
    - Area a) is the largest, with lighting, heat, wireless sockets and consumption meters, followed by b)

- The average age among the German population is increasing by the year: It was 39.3 years in 1990 and had increased to 44.5 years in 2020[12]. An older population will greatly increase the importance of Smart Home applications. For those over 65, user-friendliness is the number one requirement at 76 percent[13]. This includes:
    - User-friendly smart speakers
    - Simple set-up of new devices via QR code
    - Switch from IoT to IoTT, the "Internet of Thinking Things". This refers to "thinking systems" with autonomous decision-making.

- Our society's demographic shift is increasingly also shifting processes into the Smart Home field, such as care and assistance. In 2019, the number of people requiring care in Germany was 4.1 million, and the number is growing[14].
- The COVID-19 pandemic cause a jump in the number of people working from home from 4 percent before the pandemic to 27 percent in April 2020 during the first lockdown. In January 2021, the figure was still at 24 percent[15].
    - Due to the longer average time spent at home, the demand for consumer electronics products such as entertainment and IT devices also rose during this period[16].

[11] Source: Federal Statistical Office and ZVEI's own calculations
[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)
[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. Risk analysis

Cybersecurity can only be practically designed in relation to the intended use of the devices and applications and, therefore, the relevant associated risks. Measures will otherwise lead nowhere and waste resources. In other words, risk-based cybersecurity measures are always best. The goal is to achieve an appropriate balance between the level of protection and effort required. Conversely, this means that the risk analysis is the most important first step in any security review of products, systems or applications. It is the foundation on which all other steps and measures are based. It also ensures a realistic view of things: there is no such thing as absolute cybersecurity, and not all things can or should be highly protected.

The more intended applications there are for networked devices in a building, the higher the scale of risk will be if there is no increase in cybersecurity measures.

Object of consideration for risk analysis

A risk analysis can be conducted methodically in various ways. This white paper consciously does not single out one particular method. It is more important for the relevant aspects of a risk analysis to be clear. What is to be evaluated in a risk analysis? The following points are important key elements of a risk analysis but are certainly not an exhaustive list:

- The intended use and use environment of the device, system or application.
- The software and software libraries used in the device, system or application, including the operating system (mainly in relation to support and updates) and the hardware-specific firmware involved
- Network, protocol and communication interfaces, therefore the type of connectivity with the Internet and mobile network (direct, indirect, separate etc.)
- Backend systems and services, if present
- Delimitation to other systems and aspects that cannot be influenced
- Relevant corporate values, protection required for customer application cases must still be considered
- Organisational security in accordance with the ISO/IEC 27000-series as well as product security in accordance with IEC 62443-3-4

Structure of a risk analysis

A risk analysis should begin by identifying the relevant corporate values and processes and determining the level of protection they require. Research must then be conducted into which threats could impact these values and processes. This basic evaluation serves as the foundation of the actual risk analysis. It evaluates the probability of occurrence and damage impact of the threats to determine the overall risk (probability of occurrence x damage impact = risk). These results can be used to create an evaluation matrix and generate a risk profile for the relevant products. The end result is an overview of all products and their risks depending on the use environment and/or intended use. The risks themselves are classified and tiered in the final result. This can be done using multiple levels (e.g. high, medium or low risk).

(“high risk”: red, “medium risk”: yellow, “low risk”: green).

		Probability of occurrence				
		Rare	Unlikely	Possible	Probable	Frequent
Damage level	Trivial					
	Low					
	Moderate					
	Significant					
	Extreme					

Figure 3: Risk categorisation as per IEC 62443

The subject of this risk assessment is a service or function provided by a system or device. When any changes are made, such as in the course of a functional extension, these services or functions must be reviewed again and protected with different security measures if necessary. A device may be subject to a security risk when connected with other devices that undergo a functional enhancement that causes changes. In light of this, a complete review must be performed.

The various levels of protection aligned to the threat situation are decisive here. These protection levels define security measures to address the threat situation. The relevant application rule VDE-AR-E-2849-1, which transfers the security measures of IEC 62443 to the home area, gives recommended actions based on the corresponding protection level using basic device characteristics.

#	Object	Risk class	Reason/ derivation	Protective measure
1	Device X	low risk	Device is permanently installed in the building and has no direct or indirect connection to the Internet	a, b, c ... with Priority 1, 2 and 3
2	Device Y	medium risk	Software from third-party providers can be executed on the device	a, b, c ... with Priority 1, 2 and 3
3	Device Z	high risk	Device has IP connection and can actively execute software	a, b, c ... with Priority 1, 2 and 3

Figure 4: Example device result table as per IEC 62443

The result then serves as the basis for selecting the security measures to be implemented and their scaling. The measures are derived from the respective risk. For the specific selection of measures, various measure catalogues must be taken into account (the ISO/IEC-27000-Serie and the BSI measure catalogue for basic IT security[17]). This procedure ensures efficiency and investment security while simplifying series maintenance for the products. Moreover, this can also fulfil additional regulatory stipulations such as the product monitoring obligation included in market surveillance.

Risk analysis is not a one-off, but a continuous process.
Manufacturers must continuously monitor and evaluate both potential vulnerabilities and security incidents for their own products, the relevant application areas and supplier components.

Example case: Manufacturer X uses a software component or library from manufacturer Y in their products. If manufacturer Y announces a security hole discovered in their software, manufacturer X must be able to independently evaluate the degree to which this security hole represents a risk for their own product and which protective measures are to be initiated.

Methods for the risk analysis (example)

There are standardised procedure models, such as the one described in IEC 62443, for conducting risk analyses.

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

Generally speaking, a risk assessment should always be conducted for the respective product or application according to the security goals of confidentiality, integrity and availability – the so-called CIA triad. Structured procedure models such as STRIDE[18] help to identify common attack and manipulation opportunities in networked products and applications:

- **S**poofing (imitating, faking an identity),
- **T**ampering (counterfeiting, manipulation of data),
- **R**epudiation (limiting authentication of an action),
- **I**nformation Disclosure (openly publishing private information),
- **D**enial of Service and
- **E**levation of Privilege (unauthorised extension of rights).

A risk analysis generates added value when the results are integrated into support and product development for the next generation. This enables the efficient implementation of Security-by-Design. In addition, the company develops into a **learning organisation** for its customers.

Anchoring risk analysis in organisations

Companies can begin by entrusting people in various roles, such as product management or quality control, with the task of conducting a risk analysis. In the medium term, companies will cover these functions by forming corresponding product computer emergency response teams (P-CERT).

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

6. Basic risks for networked buildings

ZVEI member companies consider three general risks relevant for networked building environments with a view to their scalable impact – though numerous other risks certainly also exist:

1. Bot networks that impair and manipulate devices and systems
2. Destabilisation of the energy network through manipulated devices
3. Privacy violations affecting individuals or whole groups

These risks must now be traced back to their actual, product-relevant cause. Only then do they become tangible for companies. From the view of a manufacturing company, the three meta-risks listed above could be broken down as follows (this is a selection with no claim to completeness):

on 1: Modification of application software

on 2: Unauthorised access and intervention in the product

on 3: Privacy violation

Because the threat situation changes over time, it is necessary to perform a life cycle review for risks across the service life of devices for intelligent services. The risks presented above represent the requirements as determined at the present time. These must be checked based on revised threat analyses, such as those from the European Union Agency for Cybersecurity (ENISA) at European level, and the product groups and services in question in order to enable manufacturers to implement targeted security measures.

Modification of application software

The first risk is unauthorised modification of a product's application software. There is a risk that the software of a product can be manipulated or even completely replaced. This can have many different consequences. For example, a successfully manipulated product could be used as a node in a bot network for third-party criminal activities (ransomware). In practice, there are indeed many such cases in which Smart Home devices are hijacked in this manner. One example is the Mirai bot network[19], which has already been used for numerous, quite effective distributed denial-of-service (DDoS) attacks on large Internet providers. A takeover is only one possibility, though. Attacks

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

can also be carried out against devices located within communication range or against the infrastructure used to operate the device.

Unauthorised access and intervention

The second risk is unauthorised access to the product and intervention in its functions. Such attacks can induce undesired or unintended behaviour in the device that can lead to security issues or potentially even safety problems for the device itself and other connected devices. Even if the risk is considered to be low for an individual product, the risk assessment must account for the possible scalability.

Example case:

The manufacturer has a device with a load control option. If an attacker succeeds in obtaining unauthorised access to this device, they cannot do much damage in an individual device. However, if the attacker is able to sufficiently scale up this attack, they could simultaneously obtain unauthorised access to a large number of devices. In the worst case, they are then in a position to execute an attack on the power grid, for example.

Privacy violation

The third risk is violation of privacy, which entails unauthorised access to confidential and/or personal data. This is not only relevant for implementation of the General Data Protection Regulation (GDPR). The data obtained via unauthorised access can also be used improperly in other contexts. If this point is highlighted in the threat analysis, the risk must be evaluated so that it can be reduced via additional measures if needed.

Internet of Things (IoT)

The increasing number of devices directly connected to the Internet presents a particular group of risks in networked buildings. Every IoT device is a potential risk that could compromise cybersecurity. Because most devices access the Internet via local communications infrastructure, there is also a risk to this infrastructure when applications on such devices access the Internet and local resources. IP-based devices (WiFi or Ethernet) have the biggest risk potential, since they typically connect directly with cloud platforms to allow users to access the Internet. These dangers can

only be addressed in building infrastructure to a limited extent, so these devices must be reviewed in detail if they are used for services in association with other devices.

7. Basic cybersecurity measures

As described in Chapter 6, the protective measures ensuring the cybersecurity of a product or application are derived from the risks. This is always case-specific, of course, but it is possible to outline general principles and fundamental security measures that are recommended in almost all cases. This is therefore not a list of security functions, but general qualities and technology-neutral implementation options. We should mention again here that cybersecurity can only really be strengthened through the interplay of all systems, components, actors and processes (see foreword). It is not effective to only concentrate on product functions and individual manufacturers. Security by Design must go hand in hand with the secure installation and secure operation of devices and applications. If the cybersecurity of one of these aspects is compromised, this automatically jeopardises the entire security chain and renders any preceding measures ineffective.

Cybersecurity “evergreens”

Security analyses must be conducted on a case-by-case basis. This section presents brief summaries of security aspects found by ZVEI member companies to support cybersecurity and whose application should at least be considered for each product.

Cybersecurity must be taken into account across the entire building life cycle. It is the shared responsibility of all stakeholders to plan and implement the secure operation of a building. The issue of security must be incorporated into existing processes and organisational structures.

This hinges on all the people involved, who require corresponding awareness measures for their areas of activity and responsibility. Competent staff must be instructed on the guidelines and procedures in regular trainings, and this process should be documented over time. Among other things, this includes the guidelines and processes specified by the operator for implementing changes (Management of Change) and authorisation for changes to devices, work computers, servers and their connections to one another.

Security by Design in an automation solution means that security aspects must already be considered at the beginning of the planning phase. The standard IEC 62443 lays out a systematic approach for this whose principles can also be used for the automation of buildings.

It covers the following topics for implementing the technical and organisational processes that serve as the foundation for basic security coverage in building automation.

Architecture

Network security focuses on all internal and external network interfaces, which entails protecting communications against disruption, interception and manipulation as well as protecting the system network from unauthorised access. One essential measure and initial step is to segment the network. IT and building automation systems should fundamentally be separate and communication between them only allowed to the extent necessary. For example, performance-relevant control interventions (load control) should only be limited to the necessary superordinate control measures. Further network segmentation should be conducted as needed, such as according to the critical nature of operational functions, the physical or logical location, or as the result of a protection requirement or risk analysis.

System hardening

System hardening refers to the concept of having a system provide only those functions absolutely necessary for operation. The goal here is minimise the potential attack surface. Removing unnecessary programs, services, applications, nodes, authorisations, ports, access points and so on ensures that attackers and malware have fewer opportunities to compromise systems, infrastructures, firmware and applications.

Wireless networks

When wireless, Powerline[20] transmission techniques are used, their applications and intended uses must be clarified in advance. A protection requirement and risk analysis must be conducted for this scenario.

User management

User management concerns the access to a building automation system. A corresponding process must be established for this. A key principle here is minimum

[20] Technology described in the standard IEC 61131-3.

access, which dictates that only the minimum required authorisations should be granted.

Data backup and restoration

The continuous availability of systems and the data they provide is crucial for operations. To minimise potential system downtimes and the loss or damage/manipulation of data, relevant backup and recovery strategies for the building automation system should therefore be devised and installed.

Configuration and documentation

The configuration of the entire system must be defined and backed up, as well as considered in the data backup and restoration strategy. Likewise, the complete inventory and all security-relevant parameters must be consistently documented, meaning that all changes must be immediately updated in the documentation.

Protection from malware

Effective protection against malware must fundamentally consider all system components and set appropriate measures. It is not possible to install anti-virus software on many components of automation solutions (e.g. SPS, bus coupler, HMI). Selected hardening measures for the individual devices and regular installation of system and software updates or patches can already reduce the risk of a malware infection. Alternative techniques such as access-control lists, sandboxing, control of mobile devices, limiting firmware updates, continuous monitoring and the integration of monitoring tools in the automation system should be incorporated here.

Remote access

If remote access is used, the integrity and confidentiality of data as well as the authentication of communication partners must be ensured. Encrypted connections have become established as a proven security mechanism. Particularly for remote access and remote maintenance, encrypted VPN connections (e.g. via IPsec/Internet Protocol Security) can ensure the protection of integrity, confidentiality and authenticity.

Patch management

The organisational measures should include a change management process for operating the building automation system. Patch management processes should fundamentally differentiate between patches, updates and upgrades. While a patch only fixes errors, an update may introduce new functions. Installing updates therefore brings a higher risk of unwanted side effects caused by changes. For every patch or update process, companies must evaluate the extent to which the originally provided (system-wide) functionality can still be comprehensively maintained without limits. Such changes should therefore be analysed, then rolled out in a controlled manner, i.e. always with the participation of the responsible employees. If possible, changes should be verified in a test environment[21].

Control of events

In general, what counts as a security-relevant event in the system should be defined, and a process with specified procedures and responsibilities should be created. This should feature a description of how to proceed when an event occurs and which roles (or specific people) must take action.

[21] Because ZVEI does not yet have a uniform position on the topic of patch management, this section solely reflects the appraisal of the task force on cybersecurity in buildings.

8. Conclusion

Constant change is a feature of our lives and work in general and cybersecurity in particular. Social changes, technological development and even biological hazards such as a global pandemic play their role in this phenomenon. The “moving target” concept in cybersecurity is very well known at this point, but it has grown no less relevant. On the contrary, the developments of the past two years in particular have shown us which challenges exist and that they must be approached with resolve. The importance of remote work increased exponentially overnight and is expected to hold steady for the foreseeable future. It was made crystal clear to our entire society and economy that there should not and will not be any turning back on the question of digitisation and networking. Especially not if Germany wants to maintain and expand its position as an innovative business location. An appropriate level of cybersecurity is a crucial precondition for harnessing the potential of a digitised and networked world. This is the only way to discover new forms of problem solving, digital business models and cross-sector services and collaboration.

Only with innovations and comprehensive electrification and digitisation can we tackle the challenges facing our society and adapt to the coming changes. Networked buildings offer not only solution approaches to cope with the demographic shift in our society, but also the chance to make an important contribution to climate protection with higher energy efficiency and lower CO_2 emissions in the building sector.

- The status of cybersecurity as a prerequisite for digitisation poses its own challenges here.

- Cybersecurity knows no national boundaries, and technological development can and should be driven forward around the world. International standardisation is therefore indispensable for interoperability and sustainable business activities.

- Increasing levels of networking are blurring domain boundaries, and it is growing harder and harder to draw clear distinctions. The necessary requirements must be addressed through shared responsibility so that all participants do their part to secure the system.

The constant further development in terms of the threat situation, the technical and organisational measures to counter it, and general technological progress require a

constant reappraisal of this topic. Even the significantly expanded review in our white paper “Basic cybersecurity in networked buildings” only captures the situation at one moment in time, making further, continuous adjustments inevitable.

Appendix 1: Orientation aids for further research

Implementation aids:

Orientation to IoT security: ENISA Baseline Security Recommendations for IoT

Basic cybersecurity for networked (industrial) devices: BSI requirements for network-capable industrial components

Product development and product security: IEC 62443 Parts 4-1 and 3-3

Creating security levels for products and organisations: IEC 62443 Part 3-3

Secure identities: White paper on secure identities (Platform Industrie 4.0)

Basic protection: BSI guidelines on basic protection and basic IT security measures

Management system: ISO 27001

Management system for software-controlled components: VdS 3836

Cross-domain information: VDE application rule DE-AR-E 2802-20

For risk analyses/threat levels:

ENISA: Threat Landscape

BSI: Cybersecurity situation

Applicable laws:

BSI Act, amended by German IT Security Act 1 & 2

Directive on Network and Information Security (NIS Directive)

EU Cybersecurity Act

Delegated Act on Article 3 (3) d/e/f of the Radio Equipment Directive (RED) (date of application: 1 August 2024)

Currently planned legislation:

Review of the Directive on Network and Information Security (NIS-2 Directive)

Cyber Resiliance Act (CRA)/horizontal product regulation

Overviews and position papers

- ZVEI statement on the draft bill of German IT Security Act 2.0 (in German):

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

- Statement on a draft ordinance regarding an IT security mark from the Federal Office for Information Security (in German): https://www.zvei.org/themen/cybersicherheit?showPage=3208811&cHash=40f6944211f2832ea6b571854ece8975

- ZVEI white paper on horizontal product regulation for cybersecurity:

  Horizontal Product Regulation for Cybersecurity (White Paper) (zvei.org)

- BDI-DIN/DKE position paper for horizontal European cyberregulation (in German):

  Europaweite Cyberregulierung (bdi.eu)

- Orgalim position paper for horizontal product regulation for cybersecurity within the NLF:

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

- ZVEI discussion paper: Horizontal Process Requirements for the Security Life-Cycle Management of IoT Products

Appendix 2: Explanation of important basic terms

Identification: Identification refers to processes that aim to unambiguously identify a device/object. One communication partner tells the other who they are.
Authentication: Authentication refers to a process that unambiguously verifies that the right communication partner is being addressed. An addressed communication partner sends the requesting device proof that they are really authorised to exchange information with the device.

Identification and authentication ensure that the devices exchanging information are the right partners and that they are also authorised to exchange information with each other.

Roles and rights management define which actors within a system are permitted access to certain functions. A **role** contains a collection of rights and other specifications that can be assigned to one or more users. Roles must be defined in a system and then assigned corresponding qualities in terms of rights. Typical roles include user, installer, maintenance and administrator.

ZVEI: Germany’s Electro and Digital Industry Association

ZVEI represents the common interests of the electrical and digital industry and associated service companies in Germany and internationally.

This sector employs approximately 877,000 people in Germany. It generated around €200 billion in revenue in 2021.

Almost a quarter of all private-sector R&D expenditures in Germany come from the electronics industry. The industry spends some €20 billion on R&D and over €6 billion in investments annually. One-third of the industry’s turnover comes from product innovations. One in three innovations in the entire manufacturing sector originates in the electronics industry.

Basic cybersecurity in networked buildings

Version 2.0

Publisher:
ZVEI e.V.
Lyoner Straße 9
D-60528 Frankfurt am Main

Responsible:
Sanaz Khedri
Phone: +49 69 6302-222
E-mail: sanaz.khedri@zvei.org

www.zvei.org

February 2022