НАЦИОНАЛНА СИГУРНОСТ
NATIONAL SECURITY

CYBERSECURITY FOR MACHINES AND SYSTEMS

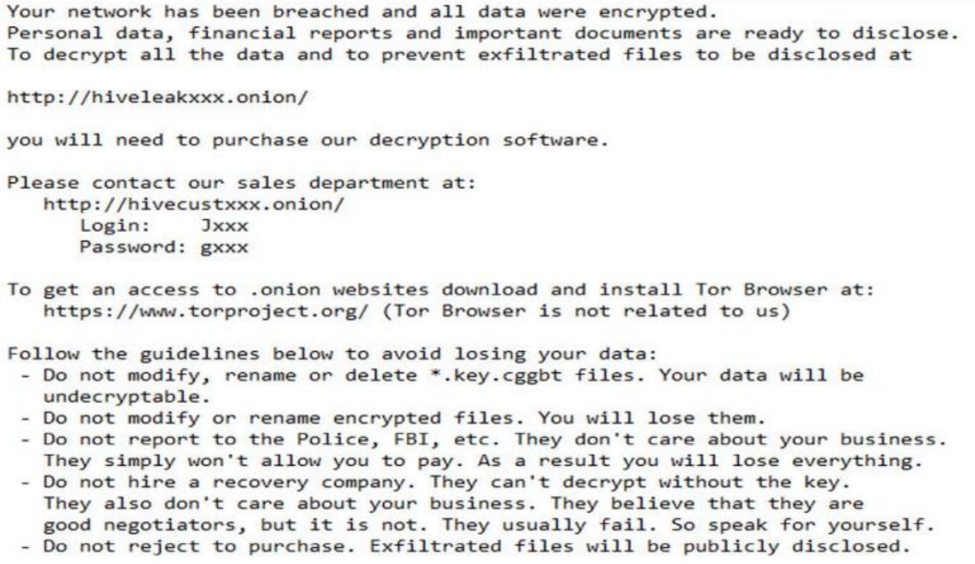
Mark Dietz
University of Library Studies and Information Technologies

Abstract: *This paper looks with cybersecurity in Germany and how it will be implemented in the future for machinery subject to inspection and using the example of lift systems. Reference is also made to the current IEC 62443 family of standards and the new Machinery Ordinance. In addition, reference is made to the Technical Rules for Operational Safety (TRBS 1115 Part 1). It also explains cybersecurity and what this means for companies and plant operators. Furthermore, various types of faults and the implementation of safety devices are considered.*

Keywords: *Cybersecurity, Cyber Resilience Act, Risk, Safety, Security, Security level*

INTRODUCTION

Technical systems are becoming increasingly digital and, thus, more vulnerable to criminal hackers. Especially systems and machines that need to be monitored are increasingly caught in the crosshairs. This is a danger to life and limb that should not be underestimated. Eleven percent of companies in Germany have fallen victim to hacker attacks in the past year, and these have repeatedly led to production downtimes. The devastating cyber-attacks have recently revealed significant security gaps in software (The State of IT Security in Germany, 2022). The following is a blackmail message from the Federal Office for Information Security (BSI) report.



```
Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.
To decrypt all the data and to prevent exfiltrated files to be disclosed at

http://hiveleakxxx.onion/

you will need to purchase our decryption software.

Please contact our sales department at:
   http://hivecustxxx.onion/
      Login:    Jxxx
      Password: gxxx

To get an access to .onion websites download and install Tor Browser at:
   https://www.torproject.org/ (Tor Browser is not related to us)

Follow the guidelines below to avoid losing your data:
 - Do not modify, rename or delete *.key.cggbt files. Your data will be
   undecryptable.
 - Do not modify or rename encrypted files. You will lose them.
 - Do not report to the Police, FBI, etc. They don't care about your business.
   They simply won't allow you to pay. As a result you will lose everything.
 - Do not hire a recovery company. They can't decrypt without the key.
   They also don't care about your business. They believe that they are
   good negotiators, but it is not. They usually fail. So speak for yourself.
 - Do not reject to purchase. Exfiltrated files will be publicly disclosed.
```

Fig. 1. Example of a blackmail message (The State of IT Security in Germany 2022, p. 16)

Due to increasing digitalization and networking, the probability of becoming a victim of a cyber-attack is constantly rising. To determine whether and to what extent cybersecurity measures are necessary, a process must be run through. This defines protection goals and a level of protection based on a risk assessment. Comprehensive process descriptions on how to proceed can be found in particular in the publications of the Federal Office for Information Security (Information security with system, 2023) and the ICS-Security-Compendium (ICS-Security-Compendium, 2013) as well as in the IEC 62443 series of standards.

At the level of European product safety, apart from a few specific areas, there are no regulatory obligations to implement cyber security measures. However, as the impact of cyber threats is now considered predictable for many products, this is changing. The new Machinery Ordinance will contain requirements obliging manufacturers to take appropriate measures to ensure that cyber threats do not compromise the product's safety (Machinery Ordinance, 2023).

The European Commission is currently working on a Cyber Resilience Act based on the IEC 62443-3-2 dated 2020 to improve the cyber security of products. In the national sphere, cyber security is also increasingly becoming the focus of occupational health and safety. Cyber security is not only an issue for the construction of new plants but also affects existing plants where cyber-attacks can lead to a risk.

WHAT IS SECURITY?

The term “cyber” is a made-up word derived from Greek cybernetics and is not without controversy due to its excessive use as a buzzword. However, since the use of the word “cyber” makes a more precise differentiation of the technology under consideration unnecessary (e.g., IT for information technology, OT for controlling systems, ICS for industrial controls) and thus has a simplifying effect as a collective term, it continues to be used in many different ways. To put it simply, Cyber.... addresses the area of technology that is characterized by changeable digital data.

Looking at cyber security in Germany, it can be seen that the threat side is constantly evolving. The number of malicious codes is increasing rapidly, and vulnerabilities in widely used systems are being exposed through cyber-attacks. The motivation behind the episodes can be both economic and terrorist. In the context of machines, it is essential to distinguish that the part of cyber security that is of interest primarily aims to protect functions. Most incidents in the public discussion occur in areas where information in the form of personal data is of value to be protected.

While it was sufficient to carry out classical error considerations (random and systematic errors) to fulfil existing safety expectations in the case of systems operating primarily in an isolated mode without a significant proportion of digital systems, the digitalization, and networking of lift systems increases the probability of occurrence and range of cyber-attacks (intentional errors) and is thus increasingly becoming a relevant threat.

However, one can face these cyber-attacks with protection. Nationally and internationally, a wealth of regulations, norms, and standards describe possible cybersecurity measures.

HOW CAN CYBERSECURITY BE IMPLEMENTED?

To answer the question, one needs the answers to three more detailed questions. The first question is: “What do I want to prevent in the first place?” the second question is: “What is my concrete need for protection?” and the third question is: “How do I realize protection?”

To clarify what I want to prevent, so-called protection goals are defined. Regarding protection goals, we can distinguish two significant areas using lift systems. The first area is the area of economic efficiency. Here, it is a question of operating a lift cost-effectively and reliably. The second aspect is the question of safety. There must be no unacceptable hazards to users or people in the vicinity of the lift system, be it by preventing an emergency call, an injury in the area of the lift doors, tripping hazards on the lift system itself, or a fall.

Once the protection goals have been defined, the components relevant to compliance with the protection goals can be identified based on the technical implementation. For the parts thus identified, often referred to as SUC (system under consideration), the next step is to determine the need for protection. This is comparable, for example, with the SIL considerations in functional safety. There are various possibilities for determining the protection requirement. The first is a simple risk matrix, in which I estimate the probability of occurrence and extent of damage for possible impacts, structure them using a matrix, and define the areas for which I must implement a specific level of cybersecurity.

Another system is contained in the IT Basic Protection Compendium (IT Basic Protection Compendium, 2023). Here, a distinction is made between different areas, basic, standard, and core protection, and for functions requiring special protection, a risk-based approach with further analyses is described. The international standard for industrial cyber security, IEC 62443, recognizes so-called security levels. These security levels describe the capabilities or resources of the attacker against whom I want to protect my system. The scale ranges from a security level of 0, corresponding to no protection, to a security level of 4, which includes protection against manipulation by comprehensive means.

The result of a protection requirement assessment is a classification of specified parts of the lift system about the need for cyber protection. This classification is then used to determine the required severity levels for the cybersecurity measures to be implemented. Depending on the set of rules used as a basis, concrete or abstract catalogues of standards or requirements are stored for specific protection needs.

The process used for implementing cyber protection always consists of comparable work steps, even across the different sets of rules. It begins in each case with the analysis of the so-called assets, which hardware, software, interfaces, processes, and so on are installed. Then, the scope of consideration is defined, for which the risks are determined based on the results of a threat analysis, and the required degree of risk reduction (protection needs assessment) is determined through cybersecurity measures. Once the measurements have been selected, they are specified and implemented for the specific use case. Once this has been done, it must then be ensured that the level of cybersecurity stays the same due to the advancing state of the art, for which suitable processes must be implemented. When changes are made to the lift system, for example, this cycle is run through repeatedly to the required extent.

For a detailed description of all necessary steps, the IEC 62443 family of standards for industrial cybersecurity can be referred to. What is particularly interesting about this family of standards is that, in addition to basic requirements from the area of management, it also describes specific procedures for the individual roles in the life cycle. There are three types of security levels to enable a suitable interaction of the existing functions about the status of protection to be achieved.

The integrator usually determines the system's security level for operation as part of his risk analysis. The information about the security level target defined as a target is made available to the component manufacturer so that he can design and manufacture his components in such a way that a security level capability is given.

The security level capability describes the ability of a component to guarantee a level of protection after it has been suitably integrated into a system. If all parts with a speaking Security level Capability are assembled according to the requirements, the fulfilment of the specified Security level Target can be proven. If this is successful, the system has achieved the planned level of protection, which is documented as Security level Achieved.

WHAT ARE THE CONTENTS OF THE REGULATIONS

Before looking at individual sets of regulations individually, it is essential to understand when rule by the legislator or the executive takes place in the first place. Every safety-oriented law is based on a hazard assessment. Risk reduction is required if hazards are unacceptable, considering the probability of occurrence and the severity of harm, as described by regulations. No mitigation measures are needed if an identified risk does not exceed the so-called risk acceptance threshold. If risk quantification is not possible, a hazard-based approach is applied. The decisive factor is the probability of occurrence, which determines whether mitigation measures are necessary.

In European product safety, two legislative projects are particularly noteworthy. The first is the so-called Cyber Resilience Act. This represents a horizontal product regulation for cyber security and describes basic requirements for all products with so-called digital elements of cyber security and the need for a risk analysis to determine the specific scope of cyber security. In addition, products are divided into classes and conformity assessment procedures are assigned to these classes according to their criticality regarding the impact of cyber-attacks. The Cyber Resilience Act does not consider only those products for which specific cybersecurity regulations are already defined in the sectoral directives.

In European product security, two legislative projects are particularly noteworthy. One of them is the so-called Cyber Resilience Act. This product regulation on cyber security describes basic requirements for all products with so-called digital elements of cyber security and the need for a risk analysis to determine the concrete scope of cyber security. Furthermore, the products are divided into classes and the effects of cyber-attacks (Cybersecurity Requirements for Products with Digital Elements and Amendment Ordinance, 2022).

In Germany, the Operational Safety Ordinance (Industrial Safety Ordinance) and now also the Act on Installations Requiring Monitoring (Industrial Safety Ordinance, 2015) apply to operators of lift systems. According to this, the operator must ensure that the systems requiring monitoring are installed, modified, and operated so that the safety and health protection of employees and other persons is guaranteed. This requires that sufficient state-of-the-art measures are defined and implemented based on a risk assessment. About possible cyber security measures, reference should be made to the Technical Regulation on Industrial Safety TRBS 1115 Part 1. This considers cyber security for safety-relevant measuring, controlling, and regulating equipment with regard to identifying and reducing hazards due to cyber-attacks within the scope of the risk assessment according to the Ordinance on Industrial Safety and Health (TRBS 1115 Part 1, 2023).

This does not mean that every lift system requires cyber security measures. Still, it is part of the obligatory risk assessment to determine whether cyber-attacks can lead to hazards in the lift system. If this is the case, suitable cybersecurity measures must be provided. Since approved inspection bodies have been commissioned under the Ordinance on Industrial Safety and Health to carry out inspections to ensure the safe operation of the system requiring review until the next check, they will no longer be able to disregard the issue of cybersecurity in the future.

CONCLUSIONS

Due to increasing digitalization, our systems are becoming increasingly vulnerable to criminal hackers. A process must be gone through to determine whether and to what extent measures are necessary. In it, protection goals and a level of protection are defined based on a cyber security risk assessment. What is cybersecurity? Cybersecurity means protecting defined functions with digital elements against cyber-attacks. Cybersecurity sets out protection objectives and defines protection levels for the assets to be protected, which, in combination, leads to the required cybersecurity measures. Due to the increasing likelihood of cyber-attacks, cybersecurity is increasingly becoming part of individual regulations at national and European levels.

Here is a reference to the new machinery regulation in Germany. For a detailed description of all necessary steps, one can refer to the IEC 62443 family of standards for industrial cyber security. In Germany, plant operators are subject to the Operational Safety Ordinance and, more recently, the Plant Act, which requires monitoring. According to these, the operator must ensure that systems requiring monitoring are set up, modified, and operated to guarantee the safety and health protection of employees and other persons. For possible cyber security measures, reference should also be made to the Technical Rules for Industrial Safety TRBS 1115 Part 1.

TRBS 1115 Part 1 considers cyber security for safety-relevant instrumentation and control systems for detecting and reducing hazards from cyber-attacks as part of the risk assessment by the Ordinance on Industrial Safety and Health.

REFERENCES

Cybersecurity Requirements for Products with Digital Elements and Amendment Ordinance. (2022). Europäische Kommission, Brüssel [viewed 06 October 2023]. Available from: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0020.02/DOC_1&format=PDF.

ICS-Security-Compendium. (2013). Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn [viewed 06 October 2023]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf? blob=publicationFile.

IEC 62443-3-2. (2020). Security for industrial automation and control systems – Part 3–2: Security risk assessment for system design. International electrotechnical commission.

Industrial Safety Ordinance. (2015). Verordnung über Sicherheit und Gesundheitsschutz bei der Verwendung von Arbeitsmitteln (Betriebssicherheitsverordnung – BetrSichV), Betriebssicherheitsverordnung vom 3. Februar 2015 (BGBl. I S. 49), die zuletzt durch Artikel 7 des Gesetzes vom 27. Juli 2021 (BGBl. I S. 3146) geändert worden ist [viewed 06 October 2023]. Available from: https://www.gesetze-im-internet.de/betrsichv_2015/BetrSichV.pdf [Accessed: 04th October 2022], Berlin: Bundesministeriums der Justiz.

Information security with system: The BSI basic IT protection. (2023). Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2023 [viewed 06 October 2023]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/sonstiges/Informationssicherheit_mit_System.pdf?__blob=publicationFile&v=3.

IT Basic Protection Compendium. (2023). Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2023. [viewed 06 October 2023]. Available from: https://www.bsi.bund.de/SharedDocs /Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1.

Machinery Ordinance. (2023). Verordung (EU) 2023/1230 des europäischen Parlaments und des Rates vom 14. Juni 2023, *Amtsblatt der Europäischen Union*, 2023 [viewed 06 October 2023]. Available from: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32023R1230.

The State of IT Security in Germany. (2022). Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2022 [viewed 06 October 2023]. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.html?nn=129410.

TRBS 1115 Teil 1. (2023). Technische Regeln für die Arbeitssicherheit – Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, 2023 [viewed 06 October 2023]. Available from: https://www.baua.de /DE/Angebote/Regelwerk/TRBS/TRBS-1115-Teil-1.html.

КИБЕРСИГУРНОСТ ЗА МАШИНИ И СИСТЕМИ

Резюме: *Настоящият доклад разглежда киберсигурността в Германия и как тя ще бъде прилагана в бъдеще за машини, подлежащи на инспекция, използвайки примера на повдигащи системи. Прави се препратка към текущия пакет стандарти IEC 62443 и новата Наредба за машините. Освен това се прави препратка към Техническите правила за оперативна безопасност (TRBS 1115, част 1). Също така се обяснява киберсигурността и какво означава това за компаниите и операторите в производствени предприятия. Разглеждат се различни видове повреди и внедряването на предпазни устройства.*

Ключови думи: *киберсигурност, Закон за киберустойчивостта, кибератаки, риск, безопасност, сигурност, ниво на безопасност, защитни цели*

Mark Dietz, PhD candidate
University of Library Studies and Information Technologies
E-mail: mark-dietz@gmx.net