IT Security Association Germany

TeleTrusT
Pioneers in IT security.

Guideline "State of the art" in IT security

Technical and organisational measures

2025

English version

In co-operation with

Acknowledgement

TeleTrusT would like to thank the following individuals for their participation in the TeleTrusT Task Force "State of the art" as well as for their active contribution in this guideline.

Project management

Tomasz Lawicki - Capgemini
RA Karsten U. Bartels LL.M. - HK2 Rechtsanwälte

Authors and participating experts

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Bartels, Karsten U. - HK2 Rechtsanwälte
Barth, Michael - genua
Bausewein, Christoph - CrowdStrike
Benzmüller, Ralf - G DATA
Bernhardt, Ulf - valantic
Dehning, Oliver - eco
Dominkovic, Dennis - SEC Consult
Dubbel, Sascha
Falkenthal, Oliver - CCVOSSEL
Fischer, Marco - procilon
Föllmer, Nancy - heinzl
Glemser, Tobias - secuvera
Gremeyer, Erik - ATM Consulting
Heyde, Steffen - secunet
Jäger, Hubert - Digital Trust Innovations
Kahrs, Malte - MTRIX
Kissling, Kristian - DCSO
Kohn, Ulrich - Adva Network Security
Kolmhofer, Robert - FH Oberösterreich
Kowol, Dominik - eperi
Krosta-Hartl, Pamela - LANCOM
Kynast, Michael - DCSO
Lang, Thomas - valantic
Lawicki, Tomasz - Capgemini
Leitner, Alexander - UNINET
Liedke-Deutscher, Bernd - TÜV Informationstechnik
Maier, Janosch - Crashtest Security
Martin, Karl-Ulrich - Detack
Menge, Stefan - Achtwerk
Mielke, Tobias - TÜV Informationstechnik
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Müller, Siegfried
Pfister, Benjamin - VAF
Rechberg, Johanna - UNINET
Rost, Peter - secunet
Schlensog, Alexander - secunet
Weigmann, Matthias - ANMATHO
Wilke, Klaus - CCVOSSEL
Zingsheim, André - TÜV TRUST IT

This document serves as a guide and provides an overview. It does not claim to be exhaustive, nor does it claim to be an exact interpretation of the existing legal provisions. It should not replace the study of the relevant directives, laws and regulations. Furthermore, the special features of the respective products and their different applications must be taken into account. In this respect, a large number of other constellations are conceivable for the assessments and procedures addressed in the document.

Imprint

Publisher:

IT Security Association Germany (TeleTrusT)
Chausseestrasse 17
10115 Berlin
Tel.: +49 30 4005 4310
E-Mail: info@teletrust.de
https://www.teletrust.de

V 1_2025-09 EN

Table of contents

Table of figures

Table index

Principles of the guidance document

Since the German IT Security Act 1.0[1] (IT-Sicherheitsgesetz, IT-SiG) was enacted in July 2015, it established the term "state of the art" (*Stand der Technik, SdT*) as a concept of fundamental importance in German information security law. The Federal Association of IT Security e.V. (*TeleTrusT*) initiated the "State of the Art" working group (*Arbeitskreis, AK*), also known as "AK SdT", to provide those affected with actionable recommendations and guidance on the required "state of the art" for technical and organizational measures. To maintain high standards, the working group has defined the following principles for the development, evaluation and updates of the guidance document:

1. **Purpose and application of the document**
   This guidance document assists organizations and vendors (manufacturers, service providers) in defining the "state of the art" within the context of applicable legislation. It can serve as a reference for contractual agreements, procurement procedures, and classification of implemented security measures.

   This guidance document is intended to be a starting point for determining which IT security measures are legally required. It does not replace technical, organizational, or legal advice. Nor can it assess security measures in individual cases. However, it can be used to identify IT security measures for bolstering system defenses against ongoing threats.

2. **Responsibility for development, evaluation and updates**
   The TeleTrusT Working Group "State of the Art" is dedicated to determining the state of the art in the context of legal standards for technical and organizational measures, while the TeleTrusT Working Group "Legal Matters" concentrates on how to implement state of the art with regards to legal requirements.

3. **A transparent process with public engagement**
   The working group develops its results through a transparent process and regularly puts the recommendations for action and guidelines up for public discussion.

4. **Evaluation method**
   The working group bases its assessment on a standardized scheme, which is completed and published for the individual measures under consideration. The method for classifying the state of art of the security measures described here is explained in Section 2 of this document.

5. **Regular updates**
   To remain current with technological advancements, this guide is intended to be updated and published regularly. Minor adjustments and additions to the guidance document (e.g. new contributions to the technical measures) will be published as revisions of the guidance document during the course of the year.

6. **Disclaimer and legal notice**
   This guidance document does not constitute a legally binding interpretation or technical standard. However, it can be used as a recognized industry consensus in professional circles, in audits, or in the interpretation of undefined legal terms. It does not replace individual legal, technical or organizational advice. Its contents are based on the current state of technology, science, and practice at the time of publication. Due to the rapid pace of legal and technical developments, this document may become temporarily outdated and require updates. The use of the recommendations in this guidance document is at your own risk.

[1] ((BSI), 2015)

1 Introduction

1.1 Legal and regulatory bases

The question of what exactly is meant by the "state of the art" in the field of information security is one of the most challenging issues in the legally compliant design and implementation of technical and organizational measures. Because these measures are crucial for the protection of network and information systems, processed data and the services offered or accessible via these network and information systems, their definitions matter.

For a long time, IT security was not strongly considered in German or European legislation. However over the past decade, German and European legislatures have started addressing the increasing digitalization of many aspects of life and the economy at the regulatory level. Since then, IT security law has been characterized by a particular dynamism that is rarely found in any other area of law. The interplay between national (implementing) legislation and European directives, the sometimes parallel existence of sector-specific and cross-sectoral regulations and the constant regulatory pressure due to technical developments and ever-evolving threat scenarios make IT security law a complex challenge for companies, public authorities, and legal practitioners alike.

To counteract this dynamic, many of the legislative acts in Germany use the phrase "state of the art" as a frame of reference and to indicate the an appropriate level of technological advancement. This concept can also be crucial for defining vague legal terms, like the "necessity" or "appropriateness" of measures. The following sections briefly outline the key laws and regulations in German IT Security law that relate to the state of the art.

1.1.1 German IT security laws and European harmonization

The European NIS directives and Germany's national IT Security Acts (IT-SiG 1.0 and IT-SiG 2.0) form the "core " of German IT security law, significantly impactingreshaping the Act on the Federal Office for Information Security (BSIG) of 2009 and introducing far-reaching regulatory changes. These regulations aim to ensure a high common level of security for network and information systems across various sectors, appropriately addressing both national and cross-border risks appropriately. The goal of the European harmonization aimsinitiative is to createestablish a consistent framework setting minimum requirements for the IT security inof network and information systems throughoutacross the entire European Union.

1.1.1.1 2015 IT-SiG

The German IT Security Act 1.0 (IT-SiG) came into force on 25 July 2015, and it marked the beginning of efforts to improve the security of information technology systems in Germany.

As an omnibus law, the IT-SiG amended various sector-specific laws. Notably, it introduced regulations for critical infrastructures (KRITIS) by revising and adding new sections to the Act on the Federal Office for Information Security (BSIG) of 2009. Additionally, it created IT security-specific amendments to several pieces of legislation, such as the Atomic Energy Act (AtG), the Energy Industry Act (EnWG), the Telemedia Act (TMG) and the Telecommunications Act (TKG).

IT-SiG implemented comprehensive revisions to the BSIG, expanding the powers and responsibilities of the German Federal Office for Information Security (BSI). For the first time, KRITIS operators were specifically addressed, and IT security obligations were imposed on them. This affected companies involved in the supply of energy, information technology and telecommunications, transport and traffic, health, water, food, and finance. The BSIG adopted a risk-based approach, targeting only those companies whose failure would pose a significant threat to essential services and public safety. This was defined by means of the threshold values in the individual sectors set by a statutory order (KRITIS Ordinance).

Under Section 8a (1) BSIG (in its prior version of 2015), KRITIS operators were required to implement appropriate technical and organizational measures to protect the availability, integrity, authenticity and confidentiality of their IT systems. The "state of the art" was already of fundamental importance as the minimum standard to be met. Additionally, the requirements included, among other things, an obligation

to provide evidence of compliance (Section 8a (3) BSIG, in its prior version of 2015) and an obligation to report certain IT security incidents (Section 8b(4) BSIG, in its prior version of 2015)
The TeleTrusT commentary on the IT Security Act and its explanatory memorandum are available at the following link: https://www.teletrust.de/it-sicherheitsgesetz.

1.1.1.2 NIS Directive

In 2016, the European Commission adopted the "Directive on measures to ensure a high common level of security of network and information systems" (NIS Directive), which had to be transposed into national law. However, this did not lead to any fundamental changes in German law, as the German legislature had already anticipated most of the European requirements by adopting the IT-SiG in 2015. The corresponding NIS Directive Implementation Act passed on 27 April 2017 and only resulted in an amendment to the BSIG.

Based on the original Directive, Section 8c BSIG (in its prior version) was established, among other things, to impose additional obligations on providers of digital services. These services include online marketplaces, online search engines and cloud computing services of a certain size. They must also implement technical and organizational measures (TOMs) to safeguard IT security, while adhering to the state of the art. The measures are intended to ensure a level of protection commensurate with the risk, covering aspects such as the security of systems and facilities, along with the management of security incidents and business continuity. Besides this, the NIS Implementation Act expanded the powers of the German Federal Office for Information Security in the BSIG. This omnibus law also amended the corresponding provisions in AtG, EnWG, SGB V and TKG.

1.1.1.3 2021 IT-SiG 2.0

The IT Security Act 2.0 (IT-SiG 2.0) came into force in May 2021, significantly expanding the existing regulations on information security in Germany.

In addition to the previously defined sectors, such as energy, water, food, health, information technology and telecommunications, transport and traffic, and finance and insurance, IT-SiG 2.0 addressed two additional areas:

- **Municipal waste disposal:** This sector, which includes the collection, transport, recovery and disposal of municipal waste, was added as a new sector of critical infrastructure.
- **Companies of particular public interest (UBI):** UBIs were added as a new target group alongside KRITIS operators and digital services providers. The UBIs include companies that are considered particularly worthy of protection due to their importance to the community. UBIs have their own set of obligations in accordance with Section 8f BSIG.

This expansion resulted in significantly more organizations being required to implement effective measures to increase their IT security.

The IT-SiG 2.0 introduced extended obligations for critical infrastructure operators and companies in the special public interest (UBI), such as:

- **Attack detection systems:** Operators are obliged to use technical tools and supporting processes for the continuous detection of threats during operation, Section 8a para. 1a BSIG. These systems must be implemented and proven in audits by 1 May 2023 at the latest.

- **Immediate registration:** Operators must register with the BSI immediately after determining their KRITIS status and designate a contact point, Section 8b para. 3 BSIG. The BSI also has the authority to independently identify operators as critical infrastructure and inspect relevant documents.

Furthermore, IT-SiG 2.0 regulated "critical components" for the first time. The use of special IT components in critical infrastructure systems must be reported to the Federal Ministry of the Interior in accordance with Section 9b (1) BSIG, which may then prohibit their use. The IT-SiG 2.0 also imposes higher fines for violations and strengthens the powers of the BSI. This allows the BSI to demand detailed access into the IT systems of the operators in the event of violations and, if necessary, mandate corrective measures.

The concept of state of the art was also been incorporated into the obligations for UBIs. The self-declaration of the UBI to be submitted in accordance with Section 8f (1) BSIG must include details on such as, how the company's IT systems are adequately protected and whether they comply with the state of

the art. However, unlike KRITIS operators, UBIs are not directly obligated to adhere to the state of the art.

1.1.1.4 NIS2 Directive

The NIS2 Directive ("Directive on measures for a high common level of cybersecurity across the Union") of 14 December 2022 is an EU directive that aims to ensure a high common level of cybersecurity within the European Union, and it replaces the NIS Directive of 2016. The deadline for Member State transposition was 17 October 2024. The German legislature has not yet met the deadline for implementation. At the time the guidance document was revised, no implementing law was available.

The NIS2 Directive expands the scope of application, overhauls the regulatory system of the original NIS Directive, and introduces stricter security requirements and reporting requirements for a wide range of sectors and companies.

Due to the restructuring of the scope, lowering of thresholds and the inclusion of new sectors, significantly more companies are subject to the NIS2 Directive than with the NIS Directive. Any company that provides critical services or has a significant societal importance will be subject to the new, stricter requirements of the NIS2 Directive.

To ensure a uniform definition and avoid differences in interpretation by Member States, the NIS2 Directive sets clear criteria for the classification of organizations. It divides affected organizations into **essential entities** and **important entities**.

According to Article 3(1) of the NIS2 Directive, the essential entities include, among others, medium to large-sized companies that can be assigned to a sector listed in Annex 1 to the NIS2 Directive (newly added sectors include wastewater, ICT services management and space). Regardless of the size of the company, qualified trust service providers and DNS service providers, among others, are also included. Public administration institutions are also regulated as essential entities. Furthermore, the scope of the NIS2 Directive also includes operators of particularly critical services, provided that they are classified as an essential entity by the Member States (see Art. 2(2)(b)-(e) NIS 2 Directive).

According to Article 3(2), the NIS2 Directive defines important entities as other companies operating in one of the sectors listed in Annex 1 or Annex 2 to the NIS2 Directive. Annex 2 encompasses sectors such as the wholesale production, industrial production or processing of food, as well as the manufacturing of goods (e.g. (in vitro diagnostic) medical devices, electronics, machinery, vehicles), and research organizations (excluding education institutions). Here, too, there is the possibility of qualification as an important entity by the Member State.

As with the NIS Directive, the obligation to take technical and organizational measures can also be found in the NIS2 Directive. These must be appropriate and proportionate, taking into account relevant European and international standards, the costs of implementation, and the state of the art, to ensure a level of security appropriate to the risk, as per Article 21(1) of the NIS 2 Directive.

Minimum requirements for risk management measures are specified in detail for the first time in the NIS2 Directive, Art. 21(2) NIS 2 Directive. There is also an increased focus on supply chain security to minimize potential vulnerabilities at third-party providers.

In addition, security incidents with significant impact must be reported immediately to the competent authorities, Art. 23 NIS2 Directive.

For a specific catalog of obligations, reference must be made to the implementing law.

1.1.1.5 NIS2UmsuCG

The law required to implement the NIS2 Directive does not currently exist. In July 2024, the Federal Ministry of the Interior published a draft law for the "NIS-2 Implementation and Cybersecurity Strengthening Act" (NIS2UmsuCG).

Essentially, the NIS2UmsuCG provided for a complete overhaul of the BSIG, which was to undergo a new regulatory structure and a considerable expansion of scope.

The draft of the new BSIG (BSIG-E) did not adopt the terminology of the NIS2 Directive, but instead distinguished between **particularly important entities** and **important entities**. In addition, **entities of**

the Federal Administration were addressed separately by the BSIG-E. Overall, the number of companies affected by the implementation draft in Germany is estimated at over 30,000.

In addition to a significant expansion of the scope of application, the BSIG-E also provided for a comprehensive program of obligations for the addressed companies: In implementation of the NIS2 Directive, companies are obliged to take the above-mentioned risk management measures and should comply with the state of the art. According to the BSIG-E, operators of critical facilities, as a subgroup of particularly important entities, must meet even stricter requirements for risk management measures. Furthermore, the BSIG-E provides for a detailed reporting system, including registration, disclosure and proactive record keeping obligations as well as implementation, monitoring, and training duties for management.

The German Federal Office for Information Security (BSI) will assume a central role as a supervisory authority and will be responsible for many new companies. The BSIG-E strengthens the powers of the BSI, in particular regarding registration and reporting obligations as well as the enforcement of security standards.

In addition to the NIS2UmsuCG, the introduction of a KRITIS umbrella law is planned, which is intended to regulate resilience and business continuity management (BCM) for operators of critical infrastructure. This law aims to increase the physical security and resilience of critical infrastructure.

Neither the NIS2UmsuCG nor the KRITIS umbrella law were ultimately implemented by the Ampelkoalition (traffic light coalition government) of the Social Democratic Party (SPD, red), the Free Democratic Party (FDP, yellow) and Alliance 90/The Greens (green), which governed Germany from 2021 to 2024. At the time of publication of this guidance document, it remains to be seen whether and what changes future implementing laws will make to the previous drafts.

1.1.2 Other European sources of law

1.1.2.1 GDPR

The European General Data Protection Regulation (GDPR) was adopted in 2016 and finally came into force on 25 May 2018. The primary goal of the GDPR is to protect the personal data of European citizens. The regulation is based on a risk-based approach regarding its protection objectives.

The state of the art is of particular importance in several areas of the GDPR.

According to Art. 25 GDPR, the principles of data protection by design (Privacy by Design) and by default (Privacy by Default) must be observed. These principles must be implemented through appropriate, risk-based technical and organizational measures.

In the area of technical data protection, risk-based and appropriate technical and organizational measures must be taken to protect the rights and freedoms of natural persons in accordance with Art. 32 (1) GDPR.

In the context of both Art. 25 para. 1 GDPR and Art. 32 para. 1 GDPR, the technical and organizational measures to be implemented must consider various aspects:

- Probability of occurrence and severity of the risk of infringement of the rights of the person concerned
- Type, scope, circumstances and purpose of the processing
- Implementation costs
- State of the art

Like IT-SiG, the GDPR does not provide a definition of what is meant by "state of the art". The same applies to the EU Data Protection Amendment and Implementation Act (DSAnpUG-EU) and the resulting new version of the Federal Data Protection Act (BDSG).

However, the state of the art must not only be taken into account as part of the implementation of the specifications, but also comprehensively documented. This has resulted in extensive documentation obligations, in particular through the obligation to carry out Data Protection Impact Assessment (DPIA) and subject to legal accountability. In this regard, the regulation stipulates documentation obligations as

separate legal obligations. Technical and organizational measures must therefore be determined individually as well as described in detail.

1.1.2.2 DORA

The Digital Operational Resilience Act (DORA) of 14 December 2022 is a European Union regulation that aims to strengthen digital operational resilience in the financial sector. In addition to the 'financial entities' listed in Article 2(1) of the DORA (credit institutions, payment institutions, trading venues, insurance and reinsurance firms, etc.), it also applies to third-party ICT service providers for those financial entities. The companies affected by the DORA had to fully implement the requirements by 17 January 2025.

DORA provides an extensive catalog of obligations. In addition to detailed obligations to implement an ICT risk management framework including strategies, procedures, protocols and tools to ensure the protection of ICT assets (Art. 5 et seq. DORA), there are also specific management, monitoring, reporting and logging obligations for the handling of ICT-related incidents (Art. 17 et seq. DORA), resilience testing obligations (Art. 24 et seq. DORA) and obligations to manage ICT third-party risk including the maintenance of a "register of information " on all ICT service contracts (Art. 28 et seq. DORA).

The state of the art is not explicitly mentioned as a legal term in the DORA. However, it is introduced by undefined legal terms: for example, by the requirements to "duly and adequately" protect all information and ICT assets (Art. 6 para. 2 DORA).

1.1.2.3 EU AI Act

With the "Regulation laying down harmonised rules on artificial intelligence" (Artificial Intelligence Act, also known as the EU AI Act) of 13 June 2024, the European Union regulated the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) for the first time. It aims to protect health, safety and fundamental rights of persons of the EU from the harmful effects of AI systems, while strengthening innovation in the field of AI through a harmonized European legal framework. The EU AI Act also takes a risk-based approach. While AI systems with unacceptable risk are generally prohibited (Art. 5 EU AI Act), "high-risk " AI systems are subject to strict requirements (Art. 6 et seq. EU AI Act). "Certain AI systems " such as those with limited risk, on the other hand, are subject to mere transparency obligations (Art. 50 EU AI Act). Largely risk-free AI systems can voluntarily adopt certain requirements and codes of conduct (Art. 95 EU AI Act). The EU AI Act addresses many different actors, some of whom are subject to overlapping and sometimes different obligations (providers, operators, importers, distributors, authorized representatives).

In addition to AI systems, general-purpose AI models (GPAI models) are also regulated by the EU AI Act, whereby GPAI models with systemic risk must meet stricter requirements (Art. 51 et seq. EU AI Act).

The state of the art can be found in several areas of the EU AI Act: When complying with the requirements for high-risk AI systems, the "*generally acknowledged* state of the art " of AI and AI-related technologies must be taken into account, Art. 8 (1) EU AI Act. Agreements between providers of high-risk AI systems and third parties in the value chain must include support obligations in accordance with the "*generally acknowledged* state of the art ", Art. 25 (4) EU AI Act. Under Art. 50 of the EU AI Act concerning transparency obligations, providers of AI systems must also "ensure their technical solutions are effective, interoperable, robust and reliable ", taking into account the "*generally acknowledged* state of the art, *as may be reflected in relevant technical standards ".* This instance is an exception, where the term is described in more detail. Finally, the "state of the art " can be found in the obligations of providers of GPAI models with systemic risk: The model assessment of providers pursuant to Art. 55 (1) (a) EU AI Act must be carried out using "standardised protocols and tools reflecting the state of the art ". The "state of the art " is also frequently mentioned in the preamble.

The EU AI Act thus impressively demonstrates how important the state of the art is as a legal concept for capturing the dynamic developments of new technologies in a legally effective manner.

1.1.2.4 EUCS

In addition, the European Commission requested ENISA (The European Union Agency for Cybersecurity) to draft the EUCS (European Cybersecurity Certification Scheme for Cloud Services) a standardized certification framework for cloud services, in accordance with Regulation (EU) 2019/881 (Cybersecurity Act). The aim is to enhance and streamline the security guarantees of cloud services through a Europe-wide harmonized security certification – especially for the public sector and in regulated markets. The EUCS supportsincludes three assurance levels ("basic", "substantial" and "high"), the requirements

for "high ", "are demanding and close to the state of the art ". Once the EUCS comes into force, it will be a cornerstone for the compliance framework for providers serving sectors such as: critical infrastructure, public authorities or the healthcare sector. This framework will help ensure state of the art practices and the trustworthiness of data processing in the cloud.

1.1.2.5 EHDS

With Regulation (EU) 2025/327 on the European Health Data Space (EHDS), the EU has adopted a new law establishing a regulatory framework for the cross-border use of electronic health data. The EHDS places high demands on technical security, interoperability and identity and access management. The EHDS implicitly incorporates the state of the art in the design of secure processing environments, identity and access management, and secure storage solutions, with detailed specification to be outlined in future implementing acts. The EHDS is strategically important for healthcare providers and IT operators, particularly when considered alongside the GDPR and sector-specific IT security laws.

1.1.3 Other relevant German laws with IT security requirements

- **EnWG:** Section 11 of the Energy Industry Act (EnWG) includes specific IT security-related obligations for operators of energy systems and energy supply networks. These sector-specific requirements take precedence over the more general requirements of Section 8a BSIG, as clarified in Section 8d (2) No. 2 BSIG. Operators are required to register, report incidents and implement a defined set of IT security catalogmeasures.catalog Additionally, they must use risk-based attack detection to continuously monitor for threats and prevent or mitigate disruptions. The use of such systems must reflect the state of the art and be regularly documented to ensure compliance and accountability.
- **AtG:** Section 44b of the Atomic Energy Act (AtG) includes a dedicated provision for IT security. It requires operators of nuclear facilities to immediately report any impairmentimpairments to their IT systems that could lead to, or have already led to, a threat or disruption affecting nuclear safety.
- **SGB V:** Section 393 of the Social Code Book V (SGB V), introduced on 1 July 2024, sets new IT security requirements for processing of health or social data in the cloud. To comply, organizations must implement *appropriate technical and organizational measures that ensure information security in accordance with the state of the art*.
- **TKG:** Section 165 of the Telecommunications Act (TKG) requires operators of public communications networks and publicly available telecommunications services to implement technical and organizational measures to protect their telecommunications and data processing systems from disruptions and risks. These measures must also reflect the state of the art as specified in Section 165 (2) sentence 3 TKG.
- **TDDDG:** Section 19 IV of the Telecommunications-Digital Services Data Protection Act (TDDDG) requires providers of digital services to implement technical and organizational measures that protect their systems from unauthorized access and disruptions. These measures must be technically feasible, economically reasonable, and aligned with the state of the art.
- **GeschGehG:** The Trade Secrets Protection Act (Geschäftsgeheimnisgesetz – GeschGehG) safeguards the rights of trade secret holders against unauthorized access, use, or disclosure of their confidential information. However, for information to qualify as a trade secret under the law, the owner must actively take appropriate confidentiality measures. What counts as reasonable depends on the circumstances of each case. Owners can implement a mix of organizational, technical and legal measures to protect the secret. When interpreting what counts as appropriate in legal terms, the state of the art can again be taken into account.

1.2 Industry-Specific Safety Standards (B3S)

According to Section 8a (2) sentence 1 BSIG, operators of critical infrastructures and their industry associations can propose industry-specific security standards (B3S) to the Federal Office for Information Security (BSI) to ensure that the requirements are met. Once submitted, the Federal Ministry of the Interior (BMI) evaluates the proposed B3S and determines whether it is appropriate for the sector.[2]

B3S are designed to support companies in implementing and proving adequate industry-specific security measures. However, the use of B3S does not change the overall scope or other requirements for the selection and maintenance of IT security measures.

Importantly, the industry-specific safety standards must also outline how to meet the state of the art in IT security over the long term, as this is a legal obligation. In practice, however, many B3S usually do not clearly define this.

Access to B3S documents is generally restricted, as most are not publicly available.

1.3 Proportionality of the measures

Various applicable laws require certain user groups to comply with or take into account the state of the art in information security[3]. However, the laws often understandably and intentionally leave room for interpretation when it comes to choosing specific security measures and criteria for doing so. This flexibility allows organizations to select security measures that are appropriate and proportionate to their specific situation, including their risk profile and financial realities.

Security measures should be selected based on a thorough risk assessment. Well-established frameworks for this include determining protection requirements using BSI IT-Grundschutz or conducting a protection needs analysis in line with ISO/IEC 27001 and related ISO 27000 standards. This guidance document offers practical suggestions to support the selection process of security measures.

While it is legally acceptable to consider cost-effectiveness when choosing security measures, organizations should also assess the efficiency and effectiveness of existing controls. In practice, this requires a tailored evaluation of your organizations existing infrastructure, application landscape, business processes, threat environment and existing security posture.

In light of this complexity, this guidance document refrains from evaluating the suitability of security measures on a case-by-case basis.

[2] Overview of industry-specific B3S at BSI: https://www.bsi.bund.de

[3] The legislation often only refers to IT security. However, the area of application must be defined more broadly when considering the protective measures specified in terms of content. For this reason, this guide considers information security as an overarching subject area.

2 Determination of the state of technology

2.1 Definition

The "state of the art" of technology[4] must be defined in terms of content separately from similar terms regarding state of technology, such as the "generally accepted rules of technology" ("GART" hereafter) and "existing scientific knowledge and research" ("ESKaR" hereafter)[5] and must be independently measurable. This distinction is the essential basis for defining the required state of technology. Many examples of how these three terms are used, both in case law and among the general public, indicate that they are either considered interchangeable, or in some cases, used incorrectly..[6]

These three terms were introduced with the Kalkar decision[7] of the Federal Constitutional Court in 1978 and the associated "three-stage theory". Based on this decision, the three technology statuses can be represented graphically roughly as follows:

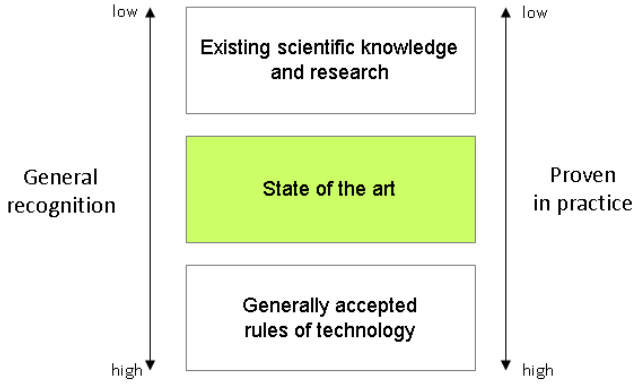


Illustration 1: Three-step theory according to the Kalkar decision

The "State of the Art" technology level is located between the more innovative "State of the Art of Science and Research" and the proven "Generally Accepted Rules of Technology" technology. These three technology statesare flanked by the categories "general recognition" and "provenin practice".

Our legal system requires a clear distinction between subjective and objective elements of anoffense. The element "state of the art" is to be understood purely objectively and technically. The subjective aspects take into account the laws in specific facts of the case. However, they do not concern the definition of the "state of the art" itself.

Thus, the "state of the art" can be described as the processes, facilities or modes of operation available in the movement of goods and services, that, when applied, can effectively ensure the achievement of the respective legal protection objectives.[8]

In short, it means that the "state of the art" refers to the best-performing IT security measure available on the market that achieves the legal IT security goal. From a technical point of view, top performance is understood to mean, in particular, the efficiency and effectiveness of safety measures.

The use of the term "prior art" in legislation strengthens the assumption that a very concrete measure is meant. In practice, however, there is not one measure that corresponds to the "state of the art" while

[4] The term "level of technology" is used as a substitute for "state of technology."
5 "Existing scientific knowledge and technology" can be used alternatively. "Existing scientific knowledge and research" will s ubsequently be used in this guide so that a distinction can be made between this and "state of the art."
6 Dr Mark Seibel, Higher Regional Court Judge, https://www.dthg.de/resources/Definition-Stand-der-Technik.pdf
[7] BVerfGE, 49, 89 [135 f]
[8] Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/ Schramm, The "State of the Art" in IT Security Law, Proceedings of the 15th German IT Security Congress 2017, German Federal Office for Information Security, 503.

other measures do not. Depending on the need for protection and the threat, there can be many solutions or bundles of measures that can be counted as state of the art.

Technical measures in the "state of the art of science and research" stage are very dynamic in their development and move to the "state of the art" stage when they reach their market launch. Nevertheless, new and innovative products can often have "teething problems" that continuously need to be resolved in short intervals and have an impact on the effectiveness of the measure.

With increasing standardization, dynamics decrease. Technical measures at the "generally accepted rules of technology" stage are also available on the market. Once they find widespread use and are frequently described in the corresponding standards, their level of innovation declines. These measures are not bad per se just because they have achieved market penetration over a longer period. However, they may have weaknesses because attackers have found ways to bypass their protection mechanisms. Sometimes, though, targeted adjustments are sufficient to restore their desired protective effect.

While the transition from "state of the art and research" to "state of the art" is relatively easy to identify through market entry, the distinction between "state of the art" and "generally accepted rules of technology" is rather difficult. In the case of technical measures, there are often new versions of a security solution or software as part of a product life cycle that are clearly localized. However, when it comes to organizational measures, it is often written standards that are referred to elsewhere as "*best practices".* They have proven themselves in practice and are hardly subject to methodological modernization.

There are also measures that are available on the market, even if their recognition by experts has decreased in terms of their effectiveness. This is the case, for example, with measures that have been compromised. Measures that are at the end of their product life cycle (EOL in PLC) and are no longer supported by the manufacturer also belong to this category. Using such measures should be avoided, since attackers can easily exploit their vulnerabilities.

Due to progress, a shift across the individual technology levels can be observed ("innovation-related shift"):

1. At its inception, a measure will initially be assigned the level of "state of science and research".
2. At market launch, it becomes "state of the art".".
3. With increasing distribution and market recognition, it will eventually achieve the level of "generally accepted rules of technology".
4. If a measure loses recognition, it can no longer be used.

In order to provide the required proof after orienting one's own measures to the state of the art, it is not sufficient to evaluate the implemented measures once and update them by installing so-called patches. Such proof can only be achieved by comparing the measures used with the alternatives available on the market at regular intervals using a transparent method.

2.2 Method for classifying the state of the art

The measures described in this guidance document were assessed using a practicable methodology based on a simple principle of answering key questions on the dimensions of "recognition by experts" and "probation in practice". These guiding questions were deliberately kept simple and allow a more detailed view of both dimensions of the investigation.

Three possible answers were given to each key question. The answers were selected in such a way that they allow classification in one of the three technological levels. Each answer must also be justified. Although the individual questions allow classification in one of the three technological levels, they each cover only partial aspects, which is why a measure's technological level is only determined after all the questions of both dimensions have been answered.

The following table shows the "State of the Art" working group's criteria for interpreting and evaluating "state of the art" measures:

- **Degree of technological recognition**

Evaluation criterion	Specification of the evaluation criterion
What **documentation** about the measure is publicly available?	Exclusively scientific publications testify to a low degree of maturity and a high degree of innovation. On the other hand, a strong presence in the mass media points to general rules of technology. Trade media are current independent media whose content is aimed at security experts.
Does the measure refer to international or national **standards**?	It's about the degree of standardization. If a measure is already mapped in national and international standards (ISO/IEC 27001ff, NIST, ENISA) and catalogs of measures (BSI TR, BSI IT-GS), it is assigned to generally accepted rules of technology. In this document, the term "set of rules" is synonymous with "norm".
Have national and international committees/associations recommended the measure?	National committees are professional associations (TeleTrusT, Bitkom, VDE, etc.) but also regulators (BSI, BNetzA, etc.). International bodies include ENISA, NIST, etc. If several committees have recommended a particular measure, it will be highly regarded in professional circles. Whereas, if a measure is not recommended by any committee, one can assume that it is still unknown.
Is the conceptual suitability of the measure independently **checked**?	When an independent body (e.g. TÜV, DEKRA, BSI, experts) regularly monitors a measure's suitability, it must have reached a high level of maturity and is therefore assigned to generally accepted rules. Measures that have not yet had their suitability independently verified lack sufficient standardization and are thus categorized as state of science and research.

- **Degree of probation in practice**

Evaluation criterion	Specification of the evaluation criterion
How should the **degree of innovation** of the measure be classified?	A measure that increases efficiency in the detection or handling of threats or introduces new approaches (innovative) in the detection and handling of threats is to be classified in th state of science and research.
Where was the current version of the measure **tested**?	Usually, the measures we consider are intended for professional use. The aim here is to distinguish between a measure that is still being developed or one that is already available on the market.
Are there **comparable** measures on the market that can achieve the required goal more effectively or efficiently?	A measure is more likely to be assigned to the state of the art in science and research if it is more efficient or more effective than all other comparable measures. On the other hand, if there are numerous alternatives (measures or bundles of measures) that can achieve the same goal, this speaks more in favor of thegenerally accepted rules of technology.
How often is the measure **conceptually updated**?	Measures with a high degree of maturity are less likely to require conceptual updates. On the other hand, less mature measures need to updated more often to conform to circumstances.

Based on a point system (1-5), an average value is derived based on the answers given. These values determine how a measure is classified as shown by the example in the following illustration:

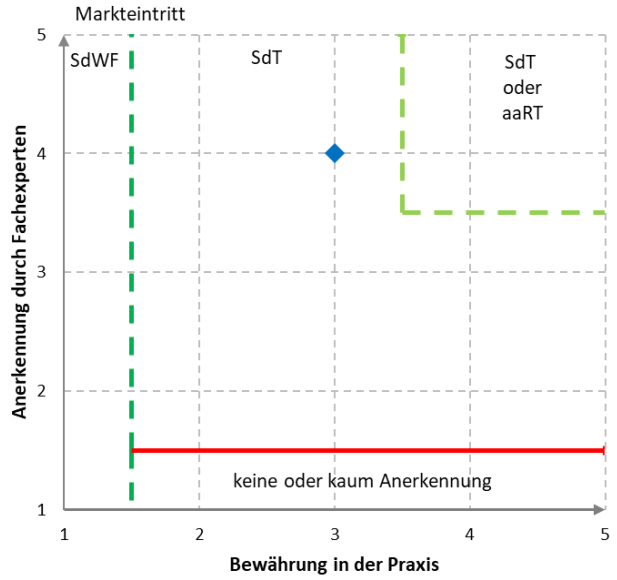


Illustration 2: Example of the classification of the state of technology

The graphic above illustrates how the "state of the art of science and research ", "state of the art" and "generally accepted rules of technology" can be classified.

The "State of Science and Research" must be positioned to the left of the market entry but may extend over the entire Y-axis due to possible recognition by experts.

If the definition of "state of the art" described above is taken as a basis, the term "state of science and research" is understood to mean processes, facilities or modes of operation whose application can tend

to ensure the achievement of the respective legal protection objectives, but whose effect has not yet been tested in practice.

With market entry, such measures reclassified as "state of the art " . They are progressive and can most effectively ensure the achievement of the respective legal protection goals.

With increasing standardization, the classification of the measure is shifted to the top right. There are tried-and-tested, standardized measures that are sufficient to meet the legal targets. They are often the basic framework of IT security but are at risk of being replaced by more advanced, efficient and effective measures. Their recognition can quickly decline, so that they find themselves at the bottom of the graph ("no or hardly any recognition").

This guidance document describes technologies and measures and classifies them according to the method described above. No security products in the strict sense are described. Therefore, for example, the suitability of any measure described here is assumed to be fulfilled for its respective purpose and validation on a case-by-case basis has not been performed.

In business practice, a suitable method (e.g., similar to the one outlined here) can be adapted to a company's existing circumstances in order to objectively evaluate the measures used, compare them with alternatives and document them for verification purposes.

2.3 Process for quality assurance of the guidance document

The "State of the Art" working group strives to ensure a high quality of the contents of the guidance document. In order for this to succeed, a process has been established in the AK SdT in which the contributions must successfully pass several stages:

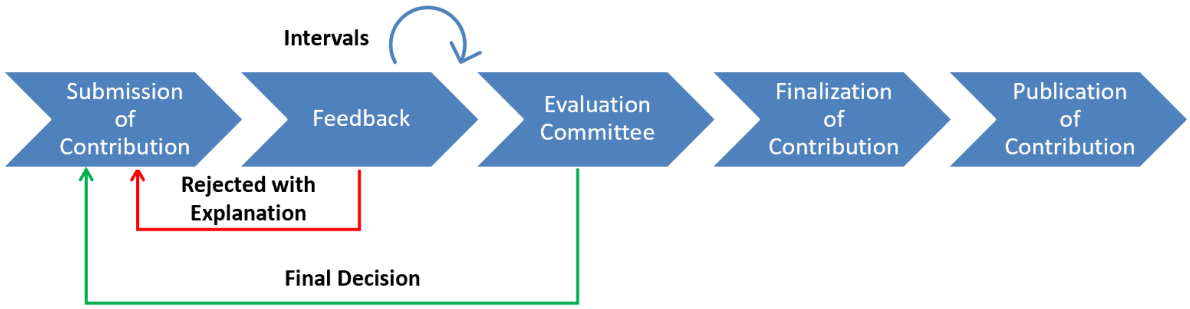


Illustration 3: Process outline for the evaluation of the measures in the working group

After submitting a new or amended contribution in a standardized template (see Illustration 3), the contribution is evaluated by IT security experts via an evaluation platform while maintaining anonymity.

The results achieved in this process are[9] discussed and finally voted on by the evaluation committee of the "State of the Art" working group, which meets regularly. The evaluation criteria include the guiding questions defined in the template and their answers, but also the technical correctness and topicality of the content.

If the evaluation committee has come to the conclusion that a contribution does not achieve the required quality, its inclusion in the guidance document will be rejected and the author will be informed of the reasons for this decision. The author then has the opportunity to update or supplement his contribution and make it available for re-examination.
Contributions that successfully pass this comprehensive procedure will be included in the guidance document.

[9] A list of the members actively involved in the TeleTrusT working group (evaluation committee) is published on the working group's website: https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/

2.4 Required protection goals

IT security pursues several protection goals to protect information and systems from threats. The three basic protection goals[10], which are also required by law, are:

- **Confidentiality**
  Confidentiality is maintained if the data worthy of protection is only made available to the authorized persons in a permissible manner.

- **Integrity**
  The integrity of the processing is ensured if no changes to the data occur unintentionally and unnoticed. To ensure integrity, the categories of consistency, accuracy, correctness and completeness must also be considered.

- **Availability**
  The availability of information technology systems and components exists if they can always be used according to their purpose and scope of functionality. To ensure availability, the categories of fault tolerance, reliability, robustness and recoverability must be considered.

In addition to these IT security protection goals focused on by the IT-SiG, there are other guarantee goals from the point of view of data protection, which are mentioned in particular due to the General Data Protection Regulation discussed here. These are, for example, non-linkability (personal data stored for multiple, non-related purposes are not linked), transparency of processing or intervenability.[11]

These additional goals are partly in competition with the previously mentioned protection goals of IT security. Since the legal requirements apply in parallel, companies must strive for a joint sustainable solution for a high level of IT security and data protection. This can only be achieved through cooperation between the IT security and data protection officers.

While from the point of view of IT security, the protection of data and infrastructure is the primary goal, data protection is about the protection of personal data. Understanding these different views is important in order to define protective measures and implement them accordingly.

[10] In addition to these three protection goals, authenticity is often also required. Authenticity is the characteristic of the authenticity, verifiability and trustworthiness of information. By authenticating the origin of the data, there can be proof that the information can be associated with a specific sender. Digital signatures make it possible to ensure the authenticity of a message.
[11] Based on the Independent State Center for Data Protection Schleswig-Holstein (ULD), https://www.datenschutzzentrum.de/

3 Technical and Organizational Measures (TOMs)

Numerous legal and normative requirements require compliance with or at least consideration of the state of the art of technical and organizational measures. There is often no further specification of the relevant systems and components. Therefore, in order to comply with the state of the art, all relevant components of data processing, including all data transmission and data storage options, must be assumed.

Since IT infrastructures are very application-dependent and industry-specific, a complete list of individual components is not possible within the framework of this guidance document. The authors have therefore focused on the description of essential components and processes.

3.1 General information

Applications are sometimes very special in the area of use in the context of the IT Security Act. This includes, for example, simple secure email communication to secure control functionality in a power plant. For this reason, it is difficult to create a complete list of applications in this publication and to describe this application. IT security can be implemented in different ways. There is more than one way to create a secure architecture. Therefore, essential points should be mentioned here that can be understood as "state of the art" in the sense of today's usability of IT security.

The respective protection requirement depends on the respective application. According to the IT Security Act, the IT security goals of integrity, authenticity, availability or confidentiality must be considered, even if they may be assessed for the individual image with different protection requirements. This means that the following protection goals in particular must be taken into account:

- Protection against attacks for unauthorized reading, modification and deletion of transmitted and stored data
- Protection against attacks on the availability of the respective services and data by the operator and user
- Protection of operating and application systems from unauthorized manipulation, etc.

In addition to the implementation of appropriate protective measures, the detection of attacks on IT systems, services and data must also be ensured in accordance with the state of the art.

Implementation should take into account the advanced procedures, whereby the use of the specific security measure or bundle of measures should be the basis of a separate protection needs analysis. Examples of security measures include:

- Multifactor authentication
- Mutual authentication
- Encryption of communication during transport
- Encryption of data (e.g., while stored)
- Securing private keys and software certificates from unauthorized duplication
- Use of secure boot processes
- Secure software administration including patch management
- Secure user administration with active locking option
- Secure mapping of network zones for additional protection at the network level
- Secure data communication between different network zones
- Safe internet browsing
- Implementation of the need-to-know principle
- Implementation of the minimal approach (including hardening)
- Implementation of logging, monitoring, reporting and response management systems
- Implementation of malware protection
- Use of secure backup systems to protect against loss of data
- Multiple design of systems to implement high availability
- Confidential data processing
- Implementation of the Zero Trust principle, etc.

In addition to individual technical application functionalities, the entire security architecture must also be considered. To this end, the following points are to be assessed within the framework of the conditions (the BNetzA requires a risk assessment high as standard or critical for critical processes and applications for the implementation of the IT security catalog in accordance with EnWG §11):

- It must be clear to the user under which conditions he can use and deploy each respective system in its corresponding secure configuration. If different application scenarios are possible on one device (e.g., access to Office-IT via Session 1 and access to Process-IT via Session 2, this must be visually apparent forto the user).

- A holistic security architecture for products and services with corresponding documentation should exist and be implemented that independent third parties can evaluate.

- The cryptography used must be modern, up-to-date and secure until the end of the product life cycle. For this purpose, the BSI recommends using only up-to-date modules with suitable algorithms.

- The product or service used must not contain any backdoors that allow data and applications to be read or manipulated.

- The manufacturer must not have access interfaces that can be used independently of the operator.

- It would be advisable to have the implementation of the security function checked by trusted third parties.

- The processes implemented in the application (e.g., user authorization, key management, etc.) must be mapped securely.

In order to evaluate a product in terms of "state of the art", addiitonal criteria must be met:

- The product or service should comply with international standards and be interoperable with standard protocols where they are used.

- If industry-specific standards exist, they should be taken into account in the application.

- The product or service must enable trouble-free operation of the components (market readiness).

- The product or service must have been successfully tested in practice.

- The evaluation must take into account that the solution must be treated as a unit if there is a coupling of hardware and software.

- The product must be securely updateable in terms of security and application functionality.

The manufacturer of the solution is also subject to criteria in the evaluation of the solution, which must be taken into account when selecting the state-of-the-art implementations. The manufacturer can guarantee investment security for the respective implementation. This means that the following checks should be carried out:

- Financial background of the manufacturer to ensure future life cycles of the product.

- There is an established product management system for the respective product and a roadmap for further development for the period of use by the user.

- The product is not labelled as a discontinued product during the period of use.

- The manufacturer reacts proactively to known vulnerabilities that affect its product, resolvesthem in a timely manner and provides necessary software updates without delay.

- The manufacturer produces the respective solution in a trusted environment with trusted personnel.

■ The manufacturer has mastered the all security functionality independently and has not become dependent on other suppliers for theirsecurity functionality.

If supplier products are used that have a lower level of trustworthiness, the security architecture of the product and measures in the production process at the manufacturer must ensure that the overall security architecture remains in place with regard to the defined protection requirements.

3.2 Technical measures

3.2.1 Authentication

A user may only access resources in the IT system if their identity has been confirmed and the rights have been verified. To do this, he logs on to the system with his user ID, which verifies his identity on the basis of factors. As a basis for authentication, a distinction is made between three categories:

- Knowledge (e.g. password)
- Ownership (e.g. tokens)
- Biometrics (e.g. fingerprint)

Knowledge-based factors include, for example, password, PIN and passphrase. Ideally, a password consists of a random string of numbers, letters and special characters. On the other hand, the personal identification number (PIN) usually consists of a 4- or 6-digit sequence of digits with which the user can identify himself on a device. Both methods are usually used in conjunction with a username. Compared to a password, a passphrase consists of several words or a longer, meaningful string of characters that is easier for the user to memorize, but which is more resistant to attacks due to its longer length.

Ownership-based factors include FIDO and OTP security tokens, as well as smartphones and classic smart cards. Security tokens are usually used to provide additional security for user accounts as a second factor, often in the form of a USB stick. They can be uniquely assigned to a user and thus personalized. Security tokens generate a One Time Password (OTP) and respond to touch or also use a biometric feature. The smartphone serves as a versatile authentication medium. For example, an OTP can be generated on the device via an authenticator application.

The third category of authentication methods is biometric factors. These include, for example, fingerprint and iris scanners as well as vein or face recognition, typing behavior and speech recognition. Of these, fingerprint and facial recognition have prevailed.

Another method is the so-called "Conditional" / "Adaptive" authentication. In this method, an authentication factor is first combined with a behavioral pattern or context analysis. Only when anomalies are detected is another factor needed for verification.

3.2.2 Assess and enforce strong passwords

This measure requires a comprehensive inventory and evaluation of all passwords, including unknown ones. This also includes simulating attacks on securely stored hash values of login data/passwords and measuring their objective resilience based on mathematical methods, personal behavior patterns, etc. The measure determines the degree of compliance with internal company guidelines and enables security-relevant measures, such as notifying employees when they use insecure passwords. This also applies to the verification of newly set passwords.

Which IT security threat(s) is the measure used against?

Unauthorized access to user accounts through:

- Guessing weak passwords by third parties
- Use of compromised passwords by third parties

What action (procedures, facilities or modes of operation) is described in this section?

Corporate and organizational networks typically use a central repository for user credentials that are used to authenticate users (e.g., Microsoft Active Directory).

If passwords are used for authentication, they are not stored in plain text, but as a hash value of the password. This prevents an attacker from gaining possession of third-party passwords through unauthorized access to password data and thus gaining access to other systems or user accounts. While this hashing functionality is a crucial protection of passwords against unauthorized access, it also prevents passwords from being evaluated in terms of their strength. However, this is necessary in order to implement appropriate measures against potential attacks, such as checking newly created passwords against dictionary words, known compromised passwords, or attempting to guess the passwords using personal information about the targeted user.

The first part of the measure, the **password security assessment**, evaluates the strength of passwords by regularly simulating real-world attacks using appropriate tools. This helps identify potential vulnerabilities such as predictable or weak passwords and flawed cryptographic implementations. The resulting metrics support the development of awareness and training initiatives, as well as their ongoing evaluation and optimization for effectiveness.

The second part involves the **enforcement of strong passwords**. This ensures that only strong and secure passwords are used. The required strength of each new password is determined by a set of rules tailored to the security level of the respective user. This level is based on the potential impact of a compromise of this account. New passwords are checked against a set of rules that match the security level, which are assigned to each account. These rules include requirements for composition (length, character sets, symbols, sequences, and repetitions), entropy (mathematical and structural), uniqueness (the password must not be used by another account within the same system in the organization), use of known default passwords, and historical password reuse.

These rules go beyond classic "blacklisting " and can be customized as needed.

At no point is plain text data is stored or displayed. If a password is rejected during a change, the user receives a personalized message explaining the reason.

Ideally, this measure is centrally managed for all systems in the organization via a single interface. This enables consistent, cross-system policy enforcement, prevents password reuse across systems, and enables centralized tracking of password history.

The described approach enables the central enforcement of appropriate password strength across the organization. It gives the organization full control, oversight, and documentation of the strength of the passwords in use. When applied regularly, these measures make it possible to assess whether the defined rules are effective or whether adjustments are needed to be ensure consistent and appropriate password strength across the organization.

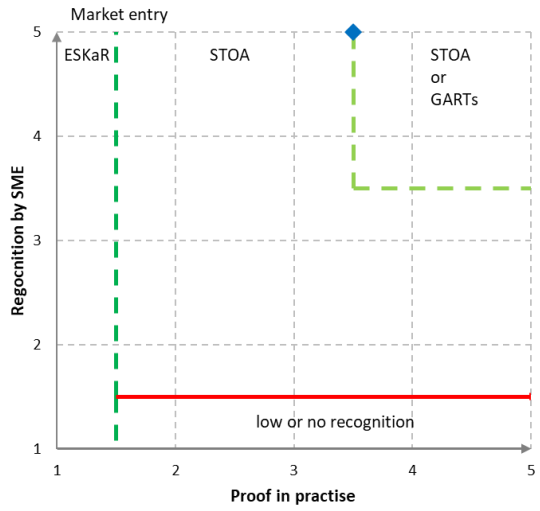
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.3 Multi-factor authentication

Multi-factor authentication (MFA) refers to the verification and validation of a user's identity using a combination of two or more authentication methods. During the login process, the user presents multiple factors such as a password and a physical security token, a password and an OTP (one-time password), or a password and a fingerprint to prove his identity (authentication, see section 3.2.1), which in turn is checked by a computer system (authentication).

Multi-factor authentication is now considered an established standard and should therefore be used wherever possible to secure identity in login processes.

Against which threat(s) of IT security is the measure used?

If a system uses only one-factor authentication, the user's identity is at greater risk of:

- Identity theft
- identity abuse
- identity fraud

One factor alone is not enough to securely authenticate user logins to computer systems, applications, or web applications. Digital attackers are becoming increasingly sophisticated, and the potential damage due to growing connectivity and digitization is becoming more severe. "Phishing", the unauthorized acquisition of login credentials (at a minimum username and password), is being dramatically professionalized by cybercriminals. Especially with the rise of artificial intelligence, phishing techniques (e.g. e-mails, fake websites, etc.) have become siginifcantly more advanced in recent years.

- Human risks in dealing with passwords:
  - Poor password quality
  - Reuse of the same password across multiple applications,
  - Intentional password sharing (e.g. sharing a common password with other people)
  - Unintentional password sharing (e.g. writing passwords down)

- Technical risks when handling access data:
    - Man-in-the-Middle (MitM) attacks
    - AI-driven and and highly professional phishing attacks
    - Keylogger-based attacks
    - Brute force attacks
    - Security vulnerabilities in applications

The use of MFA significantly reduces the risks outlined above.

What action (procedures, facilities or modes of operation) is described in this section?

MFA systems usually combine two authentication methods from different categories to form a secure authentication chain. While some MFA systems support chaining more than two methods, combining methods from the same category is not advisable. It's also important to note that not all methods across the three categories are equally secure, even in their combination.

Currently, phishing-resistant methods like passkeys, based on the FIDO2/WebAuthn standard, are considered the most secure methods. Passkeys completely replace traditional passwords with a cryptographic key pair. There are two types:

- Device-bound passkeys: Key material stored in the secure element of the end device (e.g. TPM).
- Synchronized passkeys: Kkey material is stored in a central system (e.g. cloud).

Registration typically involves of proof of device ownership (e.g. via a smartphone or computer), combined with biometric verification (e.g. fingerprint or facial recognition) or a PIN.

However, any combination, even without the use of phishing-resistant methods, is an improvement over the use of passwords alone. The combination of authentication methods can or should be chosen depending on the protection requirements of the application or user identity as well as the technical requirements.

The flexible combination of different authentication methods enables the user to use a user-friendly "password less authentication". Password less authentication can be divided into two forms:

- On the system side (technically) password-based, password less from the user's point of view A system still requires a password for authentication in the background, but this is not actively requested/required by the user in his login process

- Completely password less
  Neither from a technical nor from the user's point of view is a password required. Registration takes place without a password. As a rule, from a technical point of view, an asymmetric key method is used on the system side. The use of full password less authentication is recommended, but from today's point of view, it cannot be implemented in all grown infrastructures due to outdated software.

In addition, modern MFA systems offer a dynamic approach to user authentication (adaptive authentication). Here, the authentication method required for proof of identity, or its combination is no longer static, but situation-dependent and flexible. For example, the following characteristics can be included individually or in combination (as a risk score): group/role affiliation, geographical location of the user, speed of movement, unique device ID/device IP, typical working hours of the user, etc.

MFA can be activated in many applications today or is part of the product options. If this is not the case for applications worthy of protection or if several applications in need of protection are operated in a company, the use of a central authentication solution across all applications and users is recommended. A parallel operation of different solutions should be avoided in consideration of increasing complexity, higher costs and increased administration effort, decreasing user acceptance and increased administration effort, therefore modern MFA solutions with a centralized approach are recommended, as they offer a high degree of flexibility compared to a wide variety of authentication methods, applications, users and systems and open technical standards, such as Oauth2, OIDC, WS-Fed, SAML or REST API.
Due to the aforementioned human and technical risks of single-factor authentication, various national and international regulations such as DORA, NIS2, PSD2, KRITIS, GDPR or BAFIN require the use of MFA to secure user access to a computer system in need of protection.

When choosing a multi-factor authentication system, consider the following:

- Variety of methods:
  Support for various methods such as passkeys, one-time passwords, biometrics, and many more to meet the different needs of use cases, user groups, and roles
- Integration and compatibility:
  The MFA system must integrate seamlessly into the existing IT infrastructure in order to process logins of any kind (operating system, web-based, VPN) through open technical standards such as Oauth2/OIDC, SAML, WS-Fed, RADIUS or Web API.
- Ease of use and management:
  A centralized system for managing authentication methods that is easy to use for both administrators and end users 1. Features such as self-service options for users and detailed reports for administrators can increase efficiency and satisfaction.
- Efficient rollout processes:
  Simplify rollout processes with a centralized MFA solution with a workflow-driven registration portal that adapts to the company's layout to enable quick and easy registration of a user's methods.
- Scalability and future-proofing:
  An MFA system must be scalable to meet future requirements and technological developments for long-term effective and efficient operations.

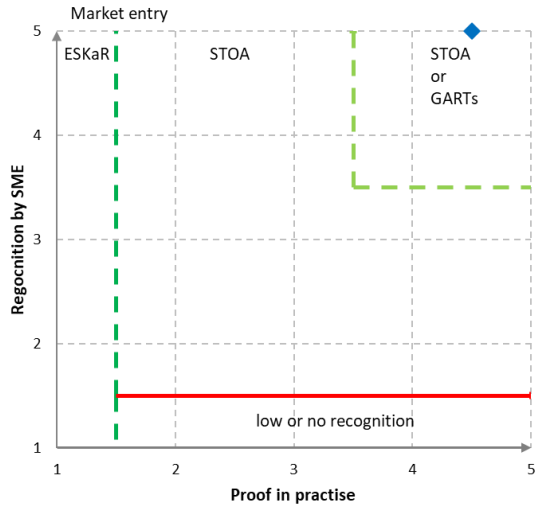
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.4 Cryptographic methods

Cryptography in the sense of information security deals with the design, definition and construction of information systems that are as resistant as possible against manipulation and unauthorized reading.

Cryptographic methods are applicable methods to protect sensitive content. The quality of the cryptographic methods depends in particular on the encryption method used (e.g. AES, ECIES), the selected key length (e.g. 512 bits), the security of the key and the implemented security configuration of the products used. As the key length increases, the number of ways to decrypt an encrypted message increases, thus increasing security.

In modern cryptography, the methods used are supposed to meet the so-called Kerckhoffs principle. This means that the security of an encryption method is based on the secrecy of the key. Therefore, the procedure used can be disclosed.

A distinction is made between symmetric and asymmetric encryption methods:

Symmetrical Procedures	**Asymmetric procedures**
▪ Complicated key distribution (if there is no secure communication channel). ▪ All participants involved in the same communication use only one, the same key. So, the same key is used for encryption and decryption. A new key must be generated for each new communication instance: N instances require keys, which correspond to quadratic growth. $\frac{(n\cdot(n-1))}{2}$ ▪ Fast encryption of bulk data. ▪ The only verifiably secure encryption method is Vernam-Cipher/one-time-pad. However, this method is hardly used in practice. ▪ Spontaneous encrypted communication without a prior relationship of trust (at least to exchange the key) is impossible unless quantum cryptography is used.	▪ For independently encrypted communication channels, the required number of keys grows only linearly with the number of participants (cf. symmetric encryption with quadratic growth). ▪ All known methods are very slow compared to symmetric encryption methods with a comparable key length. ▪ The key length required is usually longer than symmetric cryptography to provide the same security. ▪ Digital signatures are possible. ▪ Easy key exchange. There are two keys (public and private). The public key is used for encryption, while the private key is used only for decryption. Private keys are not exchanged. ▪ Not suitable for larger amounts of data.

In the hybrid process, which is usually used in practice, symmetric and asymmetric encryption are combined in order to use the advantages of the respective technology. In practice, the message to be exchanged is symmetrically encrypted with a session key. This must be large enough to prevent brute forcing of the entire key space. Then, this session key is asymmetrically encrypted with the recipient's public key and appended to the encrypted message.

With increasing technical development and the resulting increase in computing power, there is a risk that the secret key information will be determined and thus the methods used so far will be broken. This is exactly what is expected in the context of quantum computers.

To counteract this development on the encryption side, the US National Institute of Standards and Technology (NIST) has adopted three standards for quantum-resistant cryptography methods (FIPS-203[12], FIPS-204[13], FIPS-205[14]).

Regardless of this, it is recommended to check the encryption methods used regularly (e.g. annually) for their effectiveness and up-to-dateness and, if necessary, to adapt them according to current recommendations. This can be done, for example, by changing the key length (e.g. from 256 bits to 512 bits).

Against the background of the development outlined above, care must already be taken to ensure that cryptographic methods can be exchanged in the future for the protection of information that is important in the long term. This crypto agility is imperative to ensure the required level of security in the future.

[12] https://csrc.nist.gov/pubs/fips/203/final
[13] https://csrc.nist.gov/pubs/fips/204/final
[14] https://csrc.nist.gov/pubs/fips/205/final

The BSI Technical Guideline (BSI TR-02102-1) presents the encryption methods in a dedicated manner and recommends their duration of use depending on the key length used.[15] Further recommendations on tools and procedures also exist from ENISA[16].

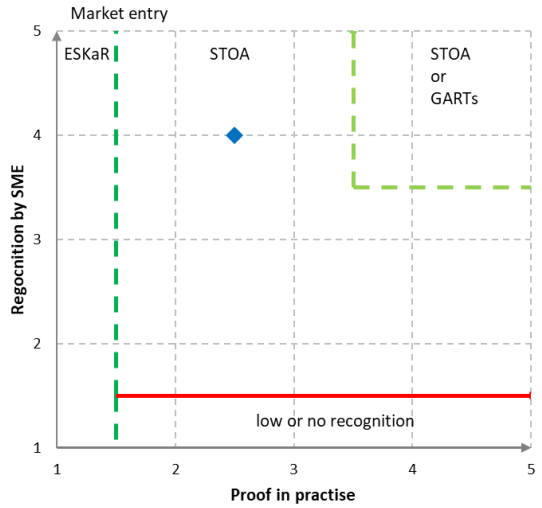
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.5 Encryption of data carriers

Full disk encryption protects the data carriers installed in a system or externally connected, such as magnetic hard drives or flash memory-based SSDs, from unauthorized access (readout, modification) by third parties. The information stored there is only accessible in plain text after manual or automated authentication of the user or computer before the PC or smartphone operating system is booted.

Against which threat(s) of IT security is the measure used?

This measure protects data on hard drives of unattended, switched off devices such as PCs, laptops, tablets or smartphones (so-called "data at rest"). In the event of loss due to inattention or theft, or temporary availability for unauthorized third parties (hotel rooms), attackers cannot evaluate or manipulate the content of the stored information. Copying the hard drives of devices protected in this way only provides useless data, as it is encrypted.

What action (procedures, facilities or modes of operation) is described in this section?

The data carrier or data carriers installed in a system, such as magnetic hard drives or flash memory-based SSDs, on which the operating system and company-confidential data are located, are encrypted by the measure in such a way that their unauthorized reading does not provide plain text. This applies both to the case of reading when the system is switched off and to a removed hard drive.
At least AES-256 should be selected as symmetric encryption in XTS mode. A central management tool makes it much easier to use on all PCs in an organization. The cryptographic keys should never, not even for backup purposes, backed up in the cloud.

[15] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html
[16] https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

In the case of full hard disk encryption, great importance should be attached to pre-boot authentication, complex passwords and 2-factor authentication, ideally by means of "knowledge and possession", for example with an additional token (see measure 3.2.3 MFA). This also enables the use of hardware-supported delay mechanisms in the event of multiple incorrect password entry.

As far as the device allows, for example with Windows 10 (and higher) systems, the so-called "Secure Boot" should also be supported. This ensures that only boot loaders with a valid signature are loaded and executed during the boot process, and thus the subsequent decryption of the operating system partition cannot be infiltrated.

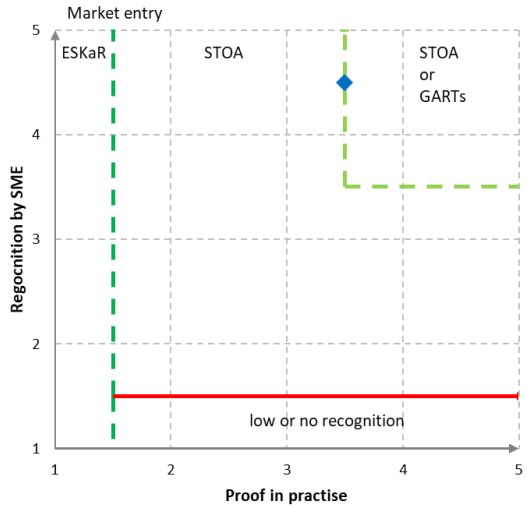
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.6 Encryption of files and folders

File and folder encryption involves the encryption of individual objects, such as containers, folders, or individual files, so this type of encryption is also known as object encryption. Object encryption offers the possibility to transport files and folders securely from one location to another and prevent unauthorized access. The programs available for this purpose decrypt the data either automatically after logging in to the operating system or after explicit user action. After that, the data is available transparently, i.e. the user can work with the objects as if they were unencrypted.

It ensures that no one except authorized people get access to protected information. This could jeopardize personal data of individuals or, in the worst case, the basis of a company's existence.

Furthermore, object encryption is a good option when using external cloud services: If the cloud operator does not have access to the encryption keys used, this can effectively prevent the operator from viewing the data. With the encryption of data in the cloud, however, there are usually restrictions regarding indexing of data, full-text search, antivirus protection or data leakage protection. These can be mitigated in part by additional, complex techniques such as the use of encryption gateways.
Against which threat(s) of IT security is the measure used?

1. interception and misuse of data during transport, e.g. by e-mail

2. Loss and theft of removable storage devices with subsequent unauthorized access to sensitive data
3. Misuse of data stored in the cloud

What action (procedures, facilities or modes of operation) is described in this section?

File and folder encryption includes the encryption of individual objects, such as containers, folders, or individual files. This allows files and folders to be transported securely from one place to another, securely stored at any location and prevented from being viewed by unauthorized persons.

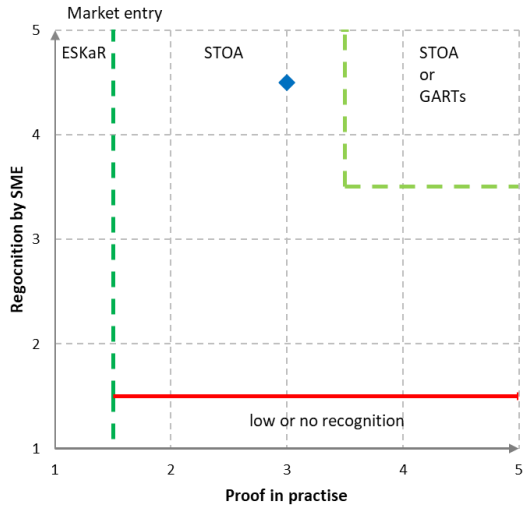
What protection goals are covered by the measure?

☐ Availability

☐ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.7 Encryption of e-mails

Business email often contains important data worth protecting. Email addresses are usually already personalized and therefore belong to the personal data that must be protected against unauthorized access or modification. The protection goals can generally be achieved by encrypting the transmission of emails and/or email content.

Against which threat(s) of IT security is the measure used?

- *Spying on or manipulating emails in transit*
- *Spying on or manipulating stored emails*

What action (procedures, facilities or modes of operation) is described in this section?

- Encrypted transmission of email (transport encryption; TLS)
- Encryption of the contents of email (S/MIME or PGP)

The security requirements for email are determined, among other things, by the type of data transmitted and stored in the email system. In business transactions, it can generally be assumed that emails contain at least important information for the company. Furthermore, e-mail addresses, if personalized, are already considered personal data; it can therefore be assumed that personal data is transmitted and

stored in emails. In individual cases and depending on the respective use of email, data may also be transmitted that require special protection, such as health data, data of clients, e.g., lawyers, or particularly valuable company secrets, such as design data.

This results in the following security requirements for email:

- Protection against unauthorized inspection or alteration of emails in transport and of stored emails (protection objective: confidentiality)
- Protection against subsequent modification of emails archived for the long term (protection objective: integrity).

These protection goals can generally be achieved through encryption. When encrypting email, a distinction must be made between encryption during transmission (transport encryption) and encryption of the email itself (also known as "end-to-end encryption"). The protection goals necessitate the use of transport encryption for sending email through public networks. However, protocols used for routing emails through the internet, namely SMTP, POP3 and IMAP, provide only unencrypted data transmission in their basic form. This is probably why most email traffic is unencrypted, although sufficient tools for encrypting email have been available for a long time.

In email traffic, TLS (Transport Layer Security) should be used for transport encryption in the currently valid version, as defined in RFC 5246. Secure encryption methods (currently e.g., AES-256) must be used, and the use of insecure encryption methods (e.g., RC4) must be excluded. Forward secrecy should generally be activated. In addition, it makes sense to check the authenticity and validity of the certificates of the respective other party used in TLS, e.g., using DANE (RFC 7671). Comprehensive recommendations on TLS are provided by the Technical Guideline TR-02102-2, Part 2 of the BSI.

End-to-end encryption is recommended for the protection of particularly sensitive data. Two standards have been established for this purpose: S/MIME (Secure/Multipurpose Internet Mail Extensions, defined in RFC 5751) and OpenPGP (Pretty Good Privacy, defined in RFC 4880). Both use basically the same cryptographic methods. However, they differ in the certification of public keys and thus in the trust models and are not compatible with each other.

When end-to-end encryption is used, no system can access the contents of an email in transit. However, this means completely dispensing with content filters, antivirus, antispam, data loss prevention and archiving. Therefore, the use of content encryption can only make sense between organizations, i.e., email are encrypted prior to entering the internet or decrypted after entering an organization’s private network (gateway) (organization end-to-end encryption.

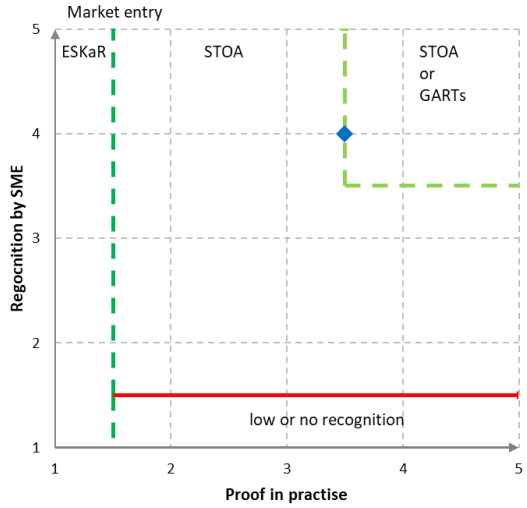
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.8 Protecting electronic traffic with PKI

In electronic data traffic, it is important that the identity of the communication partners and the authenticity of the transmitted content are ensured. The use of electronic certificates can ensure the verification of electronic identities of persons, organizations or devices. Electronic signatures are suitable for proving the authenticity of transmitted documents and messages. Certificate-based solutions are also used for secure, encrypted data transport. All these scenarios require a component for the generation, recall, management and verification of electronic certificates that ensure the validity of electronic identities in a trustworthy manner: a public key infrastructure (PKI).

Against which IT security threats is the measure used?

- Identity theft of identity / false identity
- Tampering with the contents of electronic messages or files
- Manipulating timestamps of messages or files
-

What action (procedures, facilities or modes of operation) is described in this section?

The following measures are useful against the threats described above:

- Setting up your own PKI or using an external PKI
- Use of electronic signatures (signatures, certificates, seals) of an accredited trust center
- Use of qualified timestamps to verify the authenticity and timing of messages and documents

Electronic certificates are issued by the so-called certificate authorities of PKI organizations. The term Certification Authority or CA is used here. The validity of public keys is confirmed here by digital signatures of the CA. In addition to the key itself, the digital certificate contains other information, such as its period of validity, etc. As the responsible authority, the CA is the central component in public key infrastructure. To maintain the trustworthiness of the CA, a clear verification of the identity of the applicant person or organization is necessary before the electronic certificate is issued. This is done by the Registration Authority (RA).

To verify the validity of electronic certificates, a validation service or Validation Authority (VA) is required. In general, a distinction is made between checking against a published certificate revocation list (CRL) and real-time checking by an Online Certificate Status Protocol (OCSP) service. The choice of test variant usually depends on the respective application scenario.

Depending on the legal status of the PKI, the legally usable logging of all transactions in a PKI will be useful or even necessary in most cases. Certified CA products are also required for some applications.

The possible applications of PKI-based methods are manifold. The following application methods are mentioned as examples:

- Signature and encryption of emails (S/MIME)
- IoT authentication and encryption
- Authentication and encryption on the web (HTTPS)
- Authentication and encryption for VPN services
- Authentication and encryption in wired or wireless networks (IEEE 802.1X)
- Authentication and integrity assurance of executable code (code signing)
- Authentication and integrity assurance of documents (digital signature)
- Authentication of clients/users on the internet

Depending on the status of the operator and the security standard of the associated data center, a wide variety of solutions can be set up. This ranges from a root CA, serving as a so-called root of trust, to a strictly hierarchical PKI with several subordinate CAs. Cross-certification with other PKIs is also possible.

The following diagram shows the basic structure and interaction of PKI components in a workflow.

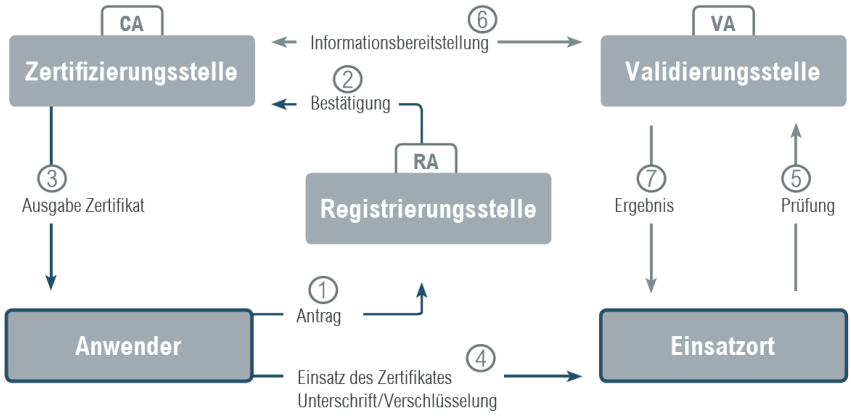


Figure 4: Structure and interaction of PKI components

The deployment of certificates is useful and helpful in almost all areas. In addition to areas of application in the public sector, they find use in the energy and public utilities sector, electronic legal transactions (with beA, beN, beBPo), healthcare, but also in the industrial and non-profit sectors (e.g. NGOs, associations, etc.).

The eIDAS Regulation in particular, provides for extensive usage scenarios. For example, identity verification and trust services are supported by PKI (see table below).[17]

eIDAS Regelungen/Anwendungfälle	
Identitäten	Zertifikate
	elektronische Ausweise
Vertrauensdienste	elektronische Siegel
	elektronische Zeitstempel
	Website-Authentifizierung
	elektronische Zustelldienste
	Bewahrungsdienste

[17] Further information can be found at https://www.ebca.de.

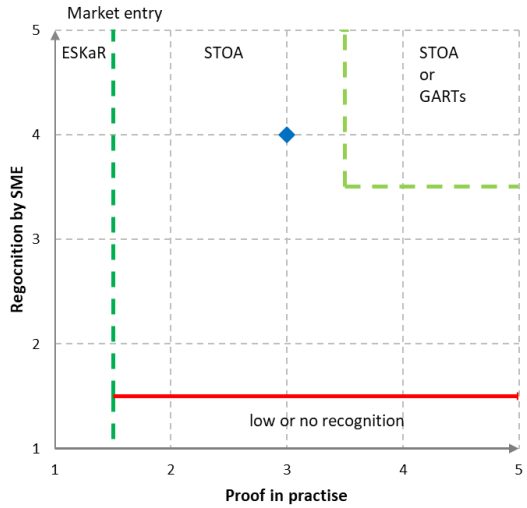
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.9 Use of encrypted VPN solutions (Layer 3)

A Layer 3 VPN refers to the connection of networks on Layer 3 of the OSI model, i.e., in particular the transport of IP data traffic within a tunnel via untrusted networks. Even if unencrypted transport were possible, it is common knowledge that VPN includes encryption. The established VPN methods are usually based on open standards or specifications such as IPSec or open-source implementations such as OpenVPN or WireGuard. The tunnel for data transport is typically established on layers 3 (IP) and 4 (TCP, UDP, ESP).

The classic use case of Layer 3 VPNs for enterprises is to provide secure network connectivity to remote offices and mobile employees. Newer applications are network overlays, e.g., in the context of multi-cloud scenarios or for connecting to cloud-based, zero-trust infrastructures. VPN services are also marketed to private customers, e.g., for using open Wi-Fi hotspots securely or circumventing GeoIP-based restrictions. Such consumer VPNs will not be considered in the following.

What IT security threats will the measure be used against?

By authenticating remote stations and encrypting data, VPNs protect against:

- Loss of confidentiality or integrity when using unencrypted or weakly encrypted connections. Or as an additional encryption layer in adefense-in-depth architecture.
- External attackers who have read access to the transported data.
- External attackers who can manipulate the transported data.

The VPNs used are also subject to other threats:

- Keys being leaked
- Weak cryptography
- Weak or incorrect authentication of remote stations
- Denial of Service: Errors or attacks jeopardize the availability of the VPN

What action (procedures, facilities or modes of operation) is described in this section?

A Layer 3 VPN refers to the connection of networks or the connection of a client to a network on Layer 3 of the OSI model. The data s in the process is encrypted and the VPN endpoints authenticate and authorize theother VPN endpoint. For example, it can be used to securely and confidentially connect company branches in different countries via insecure third-party lines, such as the internet or services rented from a telecom service provider. In contrast to a Layer 2 VPN, less data is transported because Layer 2 data, such as broadcasts, is not transmitted. In return, a Layer 3 VPN cannot be used transparently in certain (rare) application scenarios. Complex topologies, such as on-demand VPN connections, are sometimes much easier to implement with a Layer 3 VPN, or in some cases, they can only be implemented by using a Layer 3 VPN. The same applies to VPN configurations with a large number of endpoints.

A Remote Access Layer 3 VPN, in contrast to Site-to-Site VPN Layer 3 VPN, requires VPN access for each participant. Hub-and-spoke VPN architecture is often used, in this case the central node is called a VPN concentrator. Alternatives are mesh architectures in which the various participants communicate directly with each other. As a central component of an IT infrastructure, special attention must be paid to the configuration and operation of a Layer 3 VPN.

A VPN must ensure the confidentiality and integrity of the data that passes through it. To do this, the device must be able to encrypt and authenticate using algorithms and parameters that are considered secure. Whether these critical parameters are configured with sufficient security is not obvious to the user, since the VPN can often establish connections even if there are weaknesses in the configuration.

There are solid open-source implementations of VPNs that vendors often rely on for supporting their products and services. In addition to the availability of support and active patch management, commercial solutions are usually easier to configure, especially regarding patch management. Commercial solutions offer significant advantages for large and complex environments, where they can provide better protection against insecure misconfiguration, better support for high availability requirements, and integration with enterprise-specific authentication. In addition, some manufacturers offer approvals or certifications that are required for regulatory reasons in certain operating environments.

VPNs are in a critical position in the network. Errors in the manufacturer's implementation can give an attacker not only access to the communication but also access to the internal network. Unfortunately, such vulnerabilities or even explicit backdoors have not been isolated cases in the past and have also affected renowned manufacturers. Therefore, preference should be given to products that can prove a high level of platform security and a high level of self-protection, for example, through independent tests (certifications or approvals). Requirements for the operating environment must continue to ensure that physical access to the VPN devices is only possible for authorized persons.

When it comes to the protection goals of confidentiality, integrity and authenticity of the data transmitted, the integrity of the platform is also crucial. VPN devices should be built on a particularly hardened platform, have excellent self-protection, and be free of backdoors. The security protocols used by a Layer 3 VPN also guarantee the integrity and authenticity of the transported data when configured correctly.

The management and secure use of key materials also play a crucial role. In this context, solutions are to be preferred that demonstrably enable secure random number generation, secure key storage of private authentication keys (e.g., on chip cards) and track the age of encryption keys used. A particular challenge both for secure coincidence and for protection of key material is the construction of VPN endpoints in cloud environments.

To ensure the availability of the Layer 3 VPN, appropriate measures are necessary for the hardware and software of the VPN endpoint (e.g., VPN concentrators). The hardware should have redundant power supplies and fans as well as sufficient computing power. Since these measures alone are not sufficient in practice to prevent hardware failure, the possibility of redundant operation must be given (high availability configuration). Monitoring also plays a central role in ensuring that defective hardware is detected in time. Here, products should support appropriate monitoring, e.g., using SNMP. Furthermore, special attention should be paid to protection against denial-of-service attacks. Of course, a particularly secure platform is also an important prerequisite here, as is controlled access to the premises where the VPN endpoints (VPN concentrators) in the LAN are operated.

Log data accumulates on the devices of a Layer 3 VPN. These are eminently important in order to be able to detect attacks on the network. However, this data must be binding. It is also important that

administrative changes are traceable and that the log data are binding and accountable. To this end, there must be ways to store such log data in a tamper-proof manner. This can be ensured, for example, by local append-only logs or by an interface to external log servers or SIEM systems.

Note: While there is no doubt about the fundamental necessity of using VPNs, manufacturers regularly deliver innovations to increase their level of security, ease of use, and operability. The state of the art in VPNs is therefore not defined solely by their presence, but by the expression of these qualities.

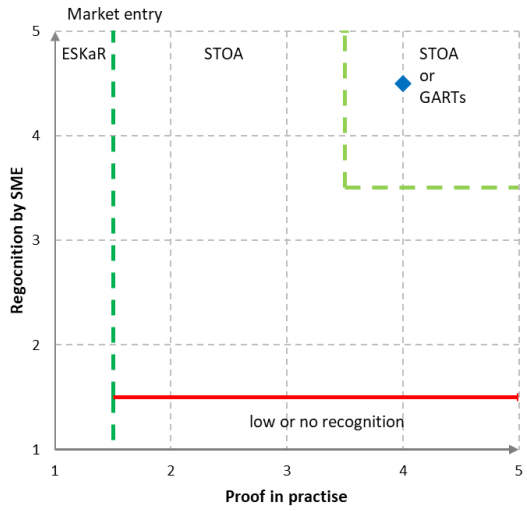
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.10 Web traffic protection

Web servers are one of the main ways malware spreads. Users are usually downloaded and executed by infected websites without them noticing. If traffic is routed through a web filter as part of a proxy server or firewall while browsing, such attacks can be detected and stopped.

Against which threat(s) to IT security is the measure used?

Web servers are one of the main ways malware spreads. Infected web servers are often used where the operator is not directly involved in the attack. A large percentage of web servers permanently have security holes and can be attacked by hackers, who then deposit malware, usually so-called root kits, on the system.

These websites are accessed normally by the user. When an infected website is visited, malware is then downloaded to the local system unnoticed by the user and activated (drive-by downloads).

In addition, specially provided web servers are used by attackers, which often imitate another web server. In the case of so-called phishing, such fake copies of well-known websites are provided with the aim of obtaining sensitive information from the user, usually their username and password, but also other personal data, liketheir bank details, credit card information, address, etc.

Often, the actual target address (URL with malicious code or the URL of the infected or fake page) is disguised by automatic redirects, often several times and via so-called URL shorteners (Bit.ly, Tiny URL,

etc.),but these are not involved in the actual attack. Users are directed to the specially provided websites through targeted links in emails, social media, etc.

What action (procedures, facilities or modes of operation) is described in this section?

To protect against such attacks, web traffic is routed through web filters. Web filters protect against these attacks by blocking the affected websites and analyzing the data loaded by websites for malicious code. Web filters can be operated centrally, as web filters in the cloud or as an on-premises appliance, or as software installed locally on the end user's system.

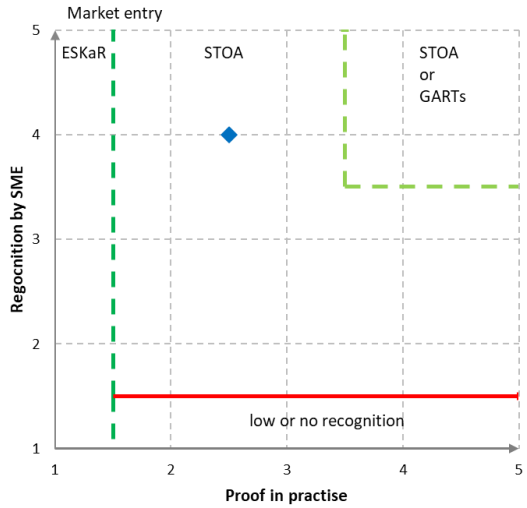
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.11 Encryption on Layer 2

Layer 2 encryption is a security solution as an alternative to Layer 3 VPNs that is applied to the payload of Ethernet frames instead of IP packets. The IP headers do not have to be processed (time savings), and bandwidth is significantly less burdened by encryption overhead than with Layer 3 encryption or higher.

Against which threat(s) of IT security is the measure used?

Recording and evaluation of massive amounts of data from inter-site traffic via the corporate network backbone or cloud connection due to security gaps in network hardware, network service providers, as well as unmonitored underground or submarine cables, and microwave or satellite connections as well as DDoS attacks on encrypted Layer 3 connections.

What action (procedures, facilities or modes of operation) is described in this section?

Secure WAN communication between corporate sites and data centers using encryption. Use of low-delay and bandwidth-neutral crypto solutions for Layer 2 WAN backbones and direct links (e.g., dark fiber, Satcom).

Layer 2 encryption is a security solution that is a convenient alternative to Layer 3 VPNs in certain application scenarios. It is applied to the payload of Ethernet frames instead of IP packets. The IP headers do not have to be processed (time savings) and there is no encryption overhead (full bandwidth is available). Its only prerequisite is an Ethernet-based network (point-to-point, hub-spoke or fully meshed) existing network cabling (copper/fiber optics) or Layer 2 services provided by network providers (e.g., carrier Ethernet services) that support special Ether types.

Typical applications for Layer 2 encryption are the protection of backbone networks (also international) and data center connections within the corporate network or to trusted cloud or colocation providers, as well as for the protection of campus WANs that run outside buildings and across third-party properties.

The performance advantages pay off especially for the introduction of central IT services, massive desktop virtualization, data center consolidation, distributed and redundant storage systems (SAN/NAS), which have a high proportion of small and/or real-time relevant IP packets (e.g., VoIP, IoT, Smart Grid), and where IPsec overhead and delay are not acceptable.

When using this network encryption technology, it is not necessary to change the existing IP routing configuration. This type of encryption is transparent to virtually all network services and applications of OSI Layer 3 (the network layer) and above, and has no measurable impact on network performance. The synchronization and authentication of the crypto counterparts, as well as the periodic change of cryptographic keys is automated. Key generation and distribution in Layer 2 crypto devices is decentralized, avoiding key servers as a single point of failure and thus increasing network availability. BSI-approved solutions are available.

MACsec is a widely used protocol for Layer 2 encryption. It is specified in the IEEE-802.1AE standard and is designed to protect Ethernet traffic from tampering and eavesdropping. The data is transmitted encrypted on the connections between neighboring network accounts (hop-by-hop encryption). Many Layer 2 encryption solutions used in practice are based on the MACsec protocol but enable end-to-end encryption.

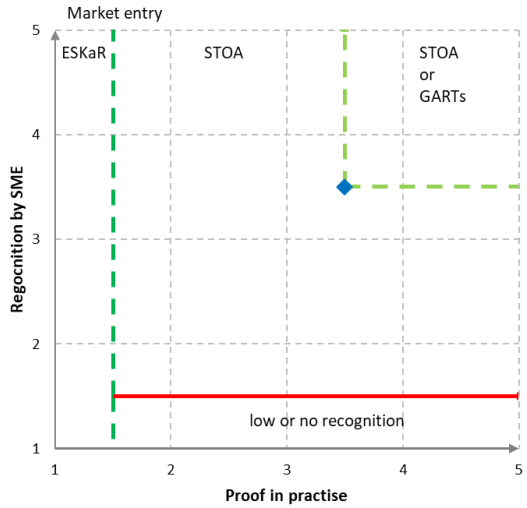
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.12 Protection of files stored in the cloud

With advancing digitalization and geographically distributed working methods, so-called cloud-based file exchange services have increasingly found application in the IT environment (e.g., Dropbox, OneDrive, Google Drive). In order to use such services safely and protect against known threats, appropriate measures must be implemented.

Against which threat(s) of IT security is the measure used?

Data stored in a cloud-based file sharing services is subject to the following threats:

- Unauthorized access and insight by the operator of the service
- Unauthorized access and inspection by third parties during processing or storage
- Unauthorized access and inspection by third parties during the transport of the data through the Internet
- Theft or unauthorized use of the identity registered with the cloud service

What action (procedures, facilities or modes of operation) is described in this section?

The following measures are useful for protecting stored data:

1. Encrypted transfer of files to and from the file exchange service
2. Encrypting data independently of the file exchange service by implementing
   a. Client-side (end-to-end) encryption of the data before transferring it to cloud storage (e.g., by encryption integrated into the data exchange service in client software belonging to the cloud storage or by separate end-to-end encryption software on the client)
   b. Gateway encryption (see the "Data storage in the cloud" chapter)

In particular, the following questions must be considered:

1. Who operates the service and does the operator have access to the data?
2. What legal disclosure/information obligations does the operator have vis-à-vis government agencies (e.g., U.S. Cloud Act)?
3. How is the data protected during processing / file storage?
4. How is the data protected during transport to and from the operator?

If the service is operated by a trusted authority, then end-to-end encryption of the data itself can be dispensed with under certain circumstances, but it is also useful in principle with trustworthy operators.

File exchange services are available in which data is transparently encrypted before upload, encrypted using client software provided by the service provider without any additional action on behalf of the user, and decrypted again after downloading. The cloud operator then only sees encrypted data. In this case, however, the operator of the file-sharing service must be trusted as the supplier of the software, or it must be confirmed that the operator does not have access to the keys used. Alternatively, client-side encryption software can be used, which ensures end-to-end encryption of the data before upload and after download. However, these solutions usually require additional effort on the part of the user. When it comes to encryption, attention should be paid to the use of secure methods for encryption, key generation and key storage.

Under no circumstances should the encryption of data be dispensed with during transport to and from the operator (transport encryption, usually TLS in the current version).

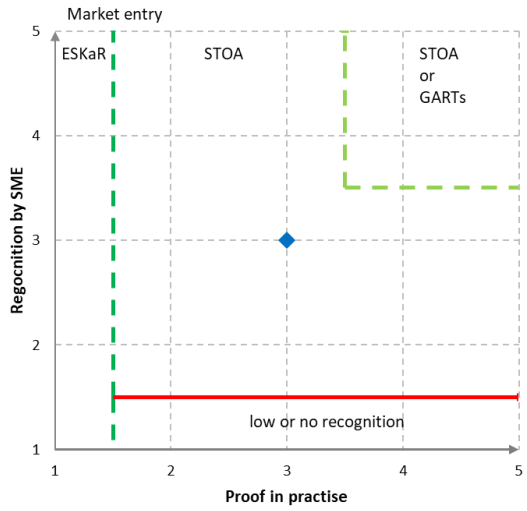
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.13 Data processing in the cloud

As soon as (highly) sensitive data leaves a secure, internal environment to be stored in the cloud, it should be encrypted before transmission, in addition to transport encryption: The encryption should remain exclusively under the control of the user organization in order to exclude unauthorized data access, even by external administrators. This is because anyone who encrypts the data (e.g. in the case of BYOK offers) automatically has access to the unencrypted data. And that should only be the user organization. A state-of-the-art solution must therefore allow for corresponding, fully internally controlled data encryption or tokenization. State-of-the-art solutions that continue to enable important functionality, such as searching or filtering data, reporting or the automated processing of encrypted data in cloud applications.

Against which threat(s) of IT security is the measure used?

Once sensitive data is transmitted to and processed by SaaS applications, it is subject to specific threats, including, in particular:

- Unauthorized access to stored or processed data by external or internal actors, such as cloud administrators.
- Interception of data in transit between the organization and the cloud (MitM attacks).
- Falsification or deletion of data during transfer to the cloud.
- Data exfiltration in the event of successful attacks on the cloud provider or via privileged access.
- Theft or unauthorized use of the identity agreed to the cloud service.

What action (procedures, facilities or modes of operation) is described in this section?

To ensure effective protection of sensitive data in the cloud, it is advisable to transmit it to the cloud application in encrypted form and process it exclusively in its encrypted state. The encryption must not restrict the functionality of the application – such as searching, filtering or evaluation.

In addition to client-side encryption (see previous chapter of this guidance document), encryption gateways provide a proven technical solution:

An encryption gateway acts as a proxy between the internal environment and the cloud application. It handles the encryption and pseudonymization of sensitive data before sending it to the cloud and decrypts returns only for authorized users. The cryptographic keys remain completely under the control of the user organization. Neither cloud providers nor their administrators have access to plain text data. By selectively encrypting or re-implementing the functionality on the encryption gateway side, relevant functions of the cloud application can still be used – e.g. searching, sorting or automated processing.

The solution used should meet the following criteria in order to be future proof:

- Key management should be able to be distributed internally to several responsible parties in order to avoid misuse and errors.
- In order to allow a consistently high level of security for all cloud applications, the solution should also be multi-cloud-capable, i.e. support several cloud providers and, depending on requirements, self-written applications in the cloud.
- In addition, the solution should support tokenization to generate format-preserving surrogate values (see corresponding chapter of this guidance document), as well as requirements for Crypto Agility (see corresponding. TeleTrusT's guidance document) to exchange algorithms if necessary.
- It should also be able to be hosted using confidential computing. Sensitive data is processed in a secure, hardware-based execution environment (Trusted Execution Environment, TEE). The data is only available in plain text within this environment, so that even system administrators do not have access to it (see also the "Cloud Security" guidance document from TeleTrusT).

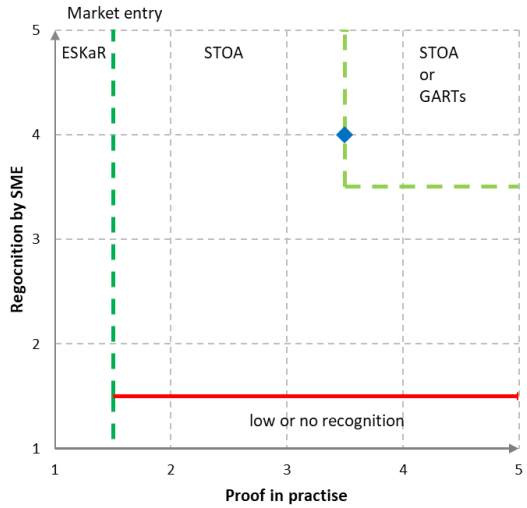
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.14 Mobile voice and data protection

Mobile phone calls and data transfers can be intercepted more easily than landline telephony. Mobile voice and data transfer encryption as well as device-side hardening and configuration protect against this.

Against which threat(s) of IT security is the measure used?

Classic landline and mobile telephony is still one of the most direct and personal communication tools today, despite chat and web conferencing applications. However, it has some dangers and offers potential attack vectors. The majority of telephone calls from landline terminals also take place with the participation of a mobile phone.

- Spying on mobile phone calls and data traffic in the network of mobile and telephony network operators, which connect the base stations with each other and the landlines and which is based, among other things, on IP technology
- Spying on mobile phone calls and data traffic and transmitting them to the attackers' command and control servers using malware installed in the mobile phone that exploits operating system and app vulnerabilities to gain direct access to the microphone, speakers, and touchscreen keyboard and screen, thereby bypassing the encryption app
- Non-encrypted mobile phone calls and data traffic can be intercepted on the air interface with low-cost hardware. To do this, attackers do not have to infect the mobile phone or break into the communication network. However, they must be in the reception area of the mobile phone in question. For example, attackers pretend to be part of the mobile network in order to get the mobile phone to be logged into their listening device and then directly record and evaluate conversations and data traffic.

What action (procedures, facilities or modes of operation) is described in this section?

The confidentiality of conversations can be ensured with the help of voice and data encryption on OSI Layer 7 (in the communication apps). Here, the spoken word as well as chat data and, if necessary, file transfers are encrypted in real time on the device and decrypted and replayed by the recipient.

The following protective measures are recommended:

- Encryption of voice and data communication by suitable and trusted apps or hardware at the application level that perform end-to-end encryption according to the current encryption standards and the applicable data protection rules
- In addition, the central configuration of the end devices by the issuing or BYOD supporting organization using mobile device management (MDM/EMM) systems to avoid unwanted user actions and app activities that can lead to mobile phone infections
- For a higher level of trust, the use of mobile phones with a hardened operating system, which ensures the exclusive use of the microphone and speaker by the encryption app, as well as preventing the spying of the crypto keys by any malware that may be present.

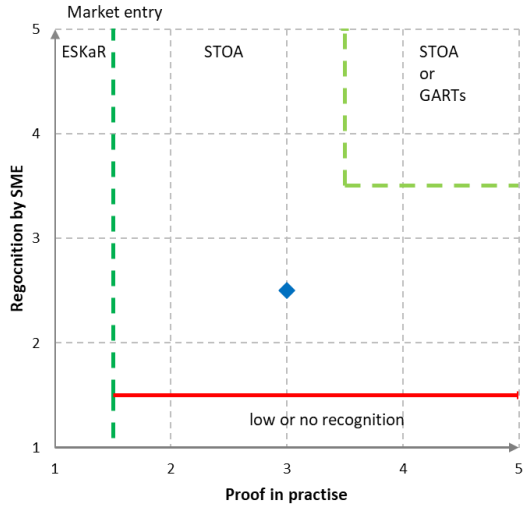
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.15 Protection of communication via instant messenger

Instant messaging is the name given to a form of digital communication in which two or more parties converse by means of quickly transmitted text, image and voice messages. To do this, the conversation partners use an instant messenger to transmit the messages over a network. If a communication partner is not online at the time a message is transmitted, it is usually delivered to the recipient at a later date. Secure instant messaging aims to protect instant messages from unauthorized access and modification.

Against which threat(s) of IT security is the measure used?

When information is exchanged via instant messaging, the following threats must be considered:

- Recording, evaluation and modification of the content by an unauthorized third party (man-in-the-middle attack)
- Identity theft within a communication system
- Theft of a device in order to be able to evaluate instant messaging data afterwards without authorization
- Unknown/Unauthorized Participants in a Group Chat

What action (procedures, facilities or modes of operation) is described in this section?

1. Secure instant messaging includes technical security measures to maintain the confidentiality and integrity of the communication content:
   - Securing message transmission using up-to-date TLS in transit
   - Use of asymmetric end-to-end encryption with security comparable to at least RSA 4096 bits
   - Forward secrecy should also be part of the architecture to protect the data from subsequent decryption despite possession of the long-term key.

2. Reliable verification / authentication of identities

3. Securing access options and access paths to the content:
   - Screen lock on the mobile device used (strong password)
   - Device encryption enabled
   - The communication app used should offer independent, secure storage of the data and protect it against extraction by unauthorized persons.

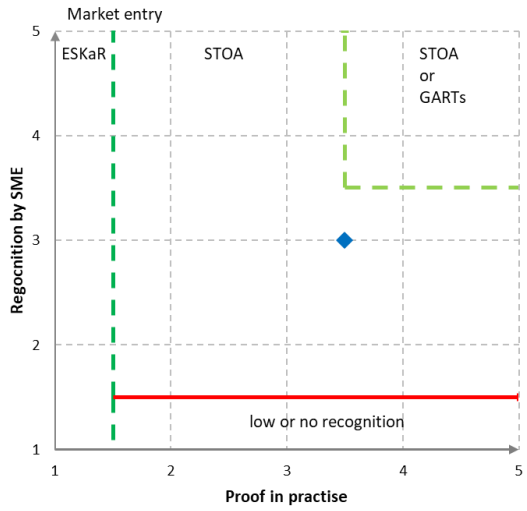
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.16 Mobile Device Protection

The use of mobile device management (MDM) solutions reduces the security risks that arise from the uncontrolled use of mobile devices for business purposes. MDM solutions make it possible to centrally administer and configure the mobile devices used.

Against which threat(s) of IT security is the measure used?

1. Data loss: If sensitive data is stored on mobile devices and the device is lost or destroyed, the company may have to accept irretrievable data loss.
2. Data theft: If a mobile device is stolen or data is leaked via insecure communication channels or applications, the confidentiality of company data is no longer guaranteed.
3. Malware: Mobile devices can be infected with malware by using public Wi-Fi networks, failing to install updates, and uncontrolled installation of applications from dubious sources.

What action (procedures, facilities or modes of operation) is described in this section?

Mobile device management (MDM) solutions enable companies and organizations to enforce policies to improve the security of devices and corporate data, among other things. MDM solutions prevent insecure communication through the use of VPNs, the secure use of Wi-Fi networks, and the use of shared applications from known sources. Device security is ensured by enforced strong authentication, compliance checks (e.g. checking system settings or permitted applications) and up-to-dateness of the operating system and installed applications. In the event of device loss, devices can be locked, and data can be wiped remotely. The protection and availability of data on the devices is achieved through the central configuration of encryption and regular data backup.

In order to meet the increased functionality requirements when using mobile devices used for business purposes, some manufacturers have expanded the existing MDM features with mobile application management (MAM) and mobile information management (MIM) functions, including cloud connection, to so-called Enterprise Mobility Management (EMM) solutions.

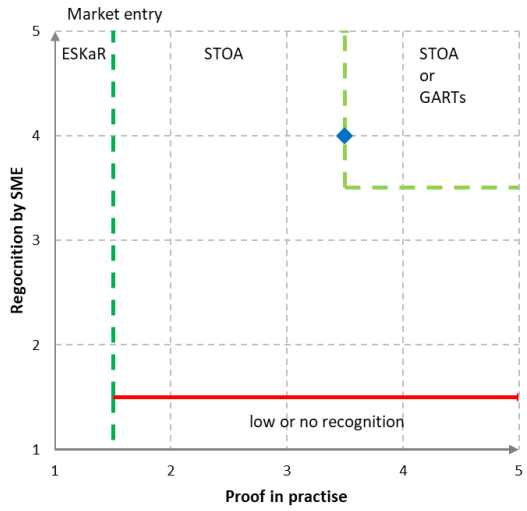
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.17 Router Security

Routers are central infrastructure components that enable the exchange of network packets between multiple networks.

In the business customer environment, routers are not only used as an Internet access device or for routing data. In most cases, they also set up VPN networks. These applications make the router a mission-critical component with specific security requirements.

The worldwide spread in both company, organizational and private networks make routers the target of various attack methods that must be fended off by appropriate protective measures. This section lists the threats to routers and describes and evaluates current protections.

Against which threat(s) of IT security is the measure used?

Routers are supposed to forward data reliably and securely and protect against unauthorized access to this data. The following threats/risks jeopardize these goals:

1. Manipulation of the configuration
2. Attacks that exploit known and unpatched vulnerabilities
3. Attacks exploiting newly discovered vulnerabilities (zero-day exploits)
4. Attacks via IP telephony connections
5. Theft (especially routers in outdoor areas / mobile communications)
6. Availability of attacks (DoS attacks)
7. Access through undocumented interfaces (so-called backdoors)
8. Executing foreign code and integrating it into botnets
9. Manipulation of routing information

What action (procedures, facilities or modes of operation) is described in this section?

There are several security measures for risk minimization for the above-mentioned threats, which can be summarized in the following as the "Router Security" bundle of measures:

1. Password protection: Use of secure access data protected from unauthorized access and avoidance of the use of standard logins
2. Regular update of router firmware
3. Service contracts with the hardware manufacturer and a defined maximum response time in the event that a serious vulnerability becomes known.
4. If a router manufacturer does not provide updates after a security vulnerability becomes known, the use of fallback devices from other manufacturers that are not affected by the vulnerability must be considered.
5. The router should be set up in an access-protected location, e.g. a lockable room with monitored access by responsible administrators. Outdoors, it is often not possible to set up the router in an access-protected location. Therefore, in such a case, the router should be equipped with a GPS function. The router should be configured in such a way that it checks whether it is still in its intended location, e.g. after a power failure. If this is not the case, he must interrupt his business.
6. To protect against DoS attacks, you should filter for invalid addresses according to RFC 2267 and block lists should be set up in the firewall.
7. All open and unneeded ports and interfaces should be closed.
8. If possible, the router should be automatically deactivated during inactivity (e.g. overnight) to reduce the attack window. The installation of updates should not be restricted by this measure.
9. In order to minimize the impact of successful attacks on routers, different network zones should be set up (network segmentation).
10. VPN router: If possible, VPN connections should not be established via pre-shared keys, but certificate-based
11. Router as VoIP gateway: Use of devices with an integrated Session Border Controller. Firewalls are not able to inspect the SIP signaling and the RTP packets with the contained voice information at the application level. This creates the risk of an attack via Voice-over-IP connections. Router operation should be monitored centrally.
12. The routing protocols used should use cryptographic methods to check received dynamic routing information and also provide outgoing routing information with authenticating information accordingly.

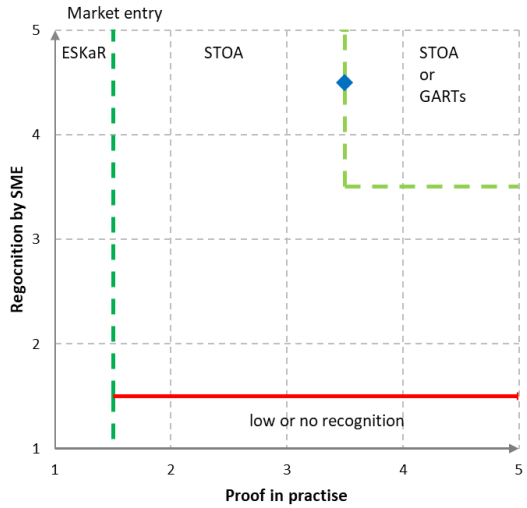
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.18 Network Monitoring with IDS

An intrusion detection system (IDS) or intrusion prevention system (IPS) is an IT system for detecting and logging potential threats in the IT/OT network, whereby the IPS also initiates defensive measures automatically.

Against which threat(s) of IT security is the measure used?

- Information leakage through interception of sensitive data
- Misuse of services and communication protocols
- Access of third-party IT systems to the IT network
- Exploitation of access options to networked IT systems
- Tampering with information or software
- Spread of malware in the IT network

What action (procedures, facilities or modes of operation) is described in this section?

An IDS or IPS detects and logs attack activity and anomalies in IT and OT networks. The goal of both systems is to detect unauthorized access and attack-typical actions (reconnaissance, lateral movement, persistence) as well as the introduction of malware as far as possible before the damage occurs. In contrast to IDS, which only displays information about suspicious or malicious activity and generates alarms, an IPS can also intervene automatically to mitigate attacks. This can be used to deal with the exploitation of specific attack vectors (such as manipulated queries that exploit a certain software vulnerability), e.g. by dropping packets at the network level. It should be noted that, for example, in industrial and production plants or fully automated ordering/delivery processes as well as message and security processes (including fire protection), direct intervention by an IPS directly affects availability and can lead to false positive detections and unwanted disturbances.

Network-based IDS / IPS systems are offered as stand-alone solutions, but also as a function of so-called UTM and Next Generation Firewalls. In the case of client/server-side IDS and IPS solutions in office IT, the functions are now also covered by modern EDR solutions (see also 3.2.22 Endpoint Detection & Response), which combine anomaly detection, process behavior, cyber threat intelligence and exploit protection.

First, IDS/IPS systems need to gain visibility in traffic. For this purpose, it is recommended for hardware-based systems to extract productive data using a test access point (TAP) in order to avoid corresponding overbooking and interpretations, as can happen with SPAN ports on switches. Network Packet Brokers (NPB) can also be used to filter the relevant data to reduce the load on the IDS / IPS. For example, they allow you to limit yourself to header/metadata or specific packet lengths. Whether header/metadata is sufficient, as well as the positioning of the IDS / IPS in the network, is based on the application.

The detection of anomalies is based on two different methods. In so-called "pattern matching", already known malware is detected on the basis of patterns (signatures) or the exploitation of a vulnerability by analyzing network packets. New attack patterns must be analyzed as quickly as possible and their signatures must be entered immediately in a tamper-proof manner, otherwise attacks based on them will remain undetected.

The second method is based on detecting changes in the communication pattern of network components by an attack. Any communication that moves outside of an expected traffic profile is considered an anomaly. This also allows new attacks to be detected. There is no need to maintain attack patterns in a database. However, it must be defined which communication patterns belong to normal data traffic. Here, the application of machine learning-supported methods helps in particular to reduce or avoid the effort required to create and maintain manual rules, provided that the quality and quantity of the training data is sufficient.

In the event of the detection of malware or an attack, or in the event of deviations from the valid target state of communication, an IDS must automatically generate corresponding event messages. All event messages should be kept in the system for a sufficiently long period of time for analysis purposes and, if necessary, exportable in an open or standardized format. The event messages must contain all relevant information for event analysis and initiation of countermeasures, such as detected signatures or conspicuous communication links. In addition, detailed network packet analyses should also be possible for further evaluations. The alarm messages should be superficially recognizable on the management

console. In addition, alarms are to be automatically sent to defined recipients and, if necessary, the detailed data on a suspected attack is to be made available via an export interface (syslog, API, webhook, etc.) to an overarching security information and event management system (see chapter "Attack Detection and Evaluation (SIEM)") for correlation and further contextual enrichment (e.g. with data from EDR systems).

An IPS should also automatically block any communication in the network that is the basis of an attack attempt. In doing so, it must be ensured that as far as possible no communication is prevented that cannot be clearly attributed to any attacking behavior.

An IDS / IPS must provide components to analyze all communication at network transitions and within internal IT networks. In the event of a temporary failure of IDS/IPS components, the data must be temporarily stored and can be merged and evaluated again after operation. No unwanted communication of the IDS / IPS components to third parties must be allowed. In addition, all IDS / IPS components in the network should not be recognizable, do not influence data traffic, do not offer any services (outside the management network) and should themselves be protected against compromise. Communication between the individual components must be confidential and with integrity.

In addition to the pure implementation of an IDS / IPS, a holistic concept for monitoring the network is also important. Network Security Monitoring (NSM) is an extension of IDS/IPS for a more comprehensive overview of all activities with associated contextual data across the network. The focus is on the provision and preparation of transaction, session and content data, which can be used for analysis of the respective event.

The data collected by IDS/IPS must be stored in such a way that it can be used for further analyses (e.g. forensics). The storage periods of the data depend on the individual specifications of the respective company.

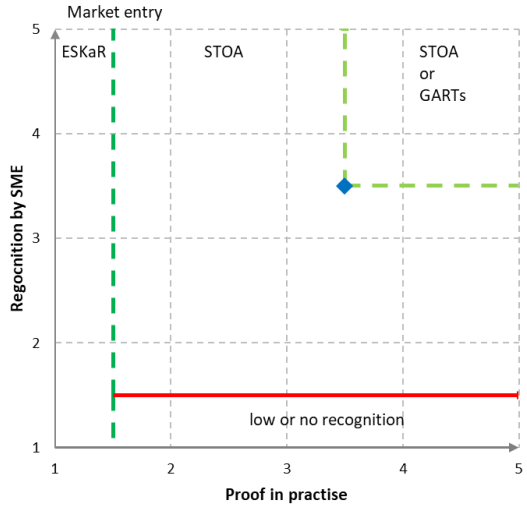
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.19 Web Application Protection

A web application firewall (WAF) protects web applications (homepages, online shops, home banking portals, etc.) from attacks. The WAF examines communication between the user and the web application at the application level and blocks potentially malicious data traffic, such as SQL injections or cross-site scripting. The term Web Service Firewall (WSF) is also used for machine-to-machine communication. Unlike a network firewall, which operates on OSI Layers 3 and 4, WAFs handle OSI Layer 7 traffic and thus protect against threats aimed at exploiting application security vulnerabilities.

Against which threat(s) of IT security is the measure used?

Attacks on web applications or web service interfaces, such as

- SQL injection
- Cross-site scripting (XSS)
- Information leakage
- Command injection
- Other OWASP threats

What action (procedures, facilities or modes of operation) is described in this section?

Use of a web application firewall (WAF or WSF) upstream of the web server.

A web application firewall (WAF) examines the communication between the user and the web application at the application level and blocks potentially harmful data traffic. In the case of security gaps in the web application that need to be closed on short notice, an adjustment of the WAF is usually sufficient. An adaptation or patching of the web application to be protected can then be planned afterwards and with sufficient lead time for tests. A combination of different vulnerabilities is often exploited for attacks. Therefore, by blocking a central vulnerability via WAF, many attacks can be quickly thwarted.

The Web Services Firewall (WSF) is a special case of the WAF for machine-to-machine communication and is also handled via http/https. The attack vectors for WAF and WSF are very similar. In the following, the same applies to the WSF as to the WAF.

Modern web applications and services often offer an application programming interface (API) that offers broad functionality for flexible machine use and is therefore rarely optimally protected.

The WAF terminates the encrypted user-side data traffic, analyzes its content, and forwards requests classified as harmless to the web server in encrypted form. Malicious requests are blocked.

The operation of web applications without the use of an upstream WAF as an appliance or virtually can no longer be regarded as state of the art.

Note: In a technical context (software development), SQL in a chat can be a normal use case and should then be adapted when configuring the WAF, based on risk.

A WAF should have the following features:

- Log data transfer to SIEM and anomaly detection systems with the option to hide passwords, credit card information, etc.
- Cluster operation capability for high availability and load balancing
- Protection against OWASP Top 10 attacks, such as SQL injection, cross-site scripting (XSS) and directory traversal via blacklisting, whitelisting and pattern recognition
- Strong authentication of web application and service users
- Session management through checking and manipulation protection of session cookies
- Broken Access Control prevents unauthorized access to paths (path traversal), files, or API functions
- Filtering unnecessary HTTP headers
- Protection against cross-site request forgery (CSRF) through header evaluation of the HTTP requests, e.g., the referrer information
- WebSocket connection protection

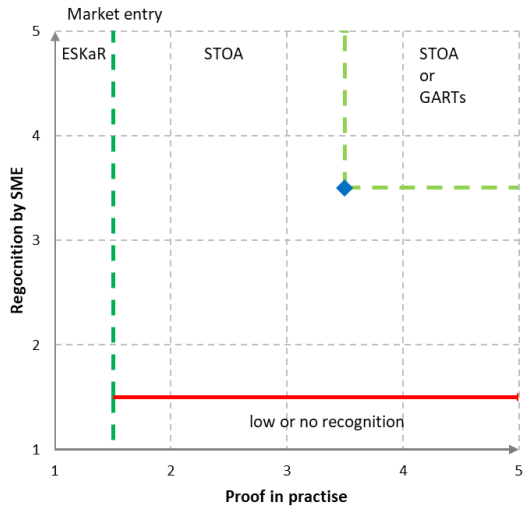
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.20 Protecting Remote Access to Networks

Remote networks must be accessible via the Internet for service or software updates. In an industrial setting, these participants are machine control components such as PLC, drive or operating devices. In the event of maintenance or software updates, the remote maintainer must access these systems online with their vendor's tools (e.g., PLC programming software).

Against which threat(s) of IT security is the measure used?

- Unauthorized access to the company network
- Unauthorized access to the target systems
- No traceability of remote maintenance access
- Data tapping or impact during a remote maintenance session

What action (procedures, facilities or modes of operation) is described in this section?

To enable remote maintenance, the target systems are typically connected to the internet via routers. These then use it to establish a VPN connection to a so-called mediation server. This exchange is the connection point between the target system and the remote operator, who has also established a VPN connection to the mediation server. Since both places have their own connection, each participant can end it at any time. The task of the mediation server is to release only the approved target systems for the respective remote operator. Ideally, it should be possible to restrict remote operators and the target system down to Layer 3 (IP, port, protocol). This ensures application-specific connections to the target system. Depending on the application, pure terminal connections can also be established via remote maintenance. These include, for example, HTTP/S, RDP, VNC or SSH access. This depends on the availability of the target system. In particular, however, a direct 1:1 network connection from the remote operator to the network of the target system should be avoided.

Encrypted connections via VPN ensure data integrity and protection against data tapping. Two-factor authentication (2FA)should be available for authorizing the remote operator.

Every remote maintenance session must be logged. This is necessary in order to be able to determine the last access to the network or router in the event of a security incident. In this case, the identifier of the remote operator (IP address, name), the time and duration of the connection should be logged. Ideally, this is stored on the mediation server.

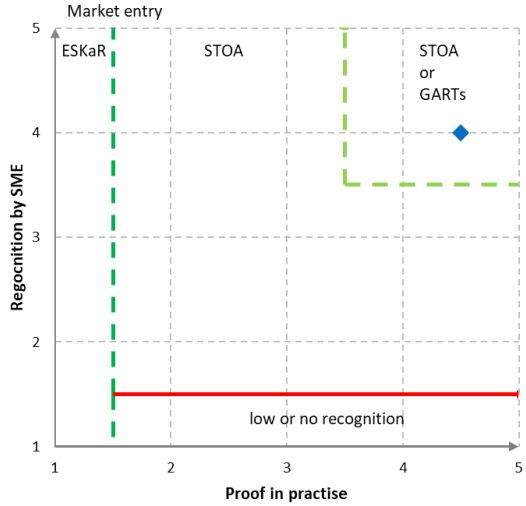
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.21 System hardening

An effective measure to reduce the attack surface of IT systems is system hardening. System hardening performs the most secure configuration of the operating system and the applications of the IT system, regardless of whether it is a physical, virtual or cloud-based. A holistic hardening approach for the entire infrastructure (on-premises and cloud) is recommended. IT systems of any kind can be hardened. This includes client and server systems in particular, but also hardware appliances (e.g., firewalls). The so-called PAW (Privileged Access Workstation), which is used as a particularly hardened client for highly privileged administration, also plays a special role.

Common operating systems (e.g., Microsoft Windows or Linux) do not have a very restrictive security configuration by default and are potentially equipped with unused components. It is precisely these unused and unconfigured functionalities that are often misused as a gateway for attackers. During system hardening, these functionalities and their interfaces are switched off or restricted and a strong security configuration is established. This significantly increases the security of the systems. Therefore, system hardening should be an integral part of a company's technical security strategy.

Against which threat(s) of IT security is the measure used?

The main threats to non-hardened systems are:

- Data manipulation of personal data and sensitive company data
- Data extraction(e.g., data dumps of entire databases from database systems)
- Manipulation or sabotage of operating and production processes as well as disruption of operational functions (e.g., DDoS)
- Identity theft (e.g., taking over highly privileged accounts or service accounts)

- Introduction of malware of any kind and distribution of the malware to other systems (including ransomware)
- Misuse of system resourcs for the attacker's processes (e.g., crypto mining, spam sending)
- Exploitation as an initial foothold in the network for attackers to then attack other systems (e.g., lateral movement, supply chain attack)

What action (procedures, facilities or modes of operation) is described in this section?

The following measures must be taken into account in particular for the hardening of systems:

1. Disabling components
    - Regular review of whether activated services are still necessary for operation
    - Deactivate or uninstall unnecessary operating system components/services, including background services
    - Uninstall unnecessary software
    - Disable unnecessary autostart or scheduled processes
    - Deactivate unneeded, technically outdated or insecure interfaces or protocols
    - Deactivate transmissions (e.g., telemetry data), unless they are required for central monitoring with a coordinated policy
    - Disable unused file shares
    - Deactivate or limitate access to administrative websites
    - If necessary, disable unneeded ports or other physical interfaces
    - If necessary, deactivate or limit the privileges of accounts that are not needed
    - Special monitoring for dual-use tools for covert activities ("LOL-bins") - also in the cloud.

2. Enable hardware-level protection

    - Enable CPU security features and check that applications are working properly (e.g., Address Space Layout Randomization "ASLR", Data Execution Prevention "DEP", Control Flow Guard "CFG")
    - Activate the BIOS access password, limitation of the boot sequence to the necessary devices
    - If necessary, activate protection procedures against side-channel attacks
    - If necessary, activate secure boot procedures

3. Security
    - Use of communication protocols to ensure that sensitive data and authentication information are transmitted in encrypted form
    - Use of certificates to exchange cryptographic keys
    - Deactivate autostart mechanisms (e.g., for USB media)
    - Enable a screensaver with password protection
    - Enable strong user account control (e.g., Windows User Account Control)
    - Enable anti-malware protection on the system during the boot process (Secure Boot)
    - Remove unnecessary certificates from trust stores
    - Hide references to installed services or version numbers
    - Disable error or debug messages for end users or replace them with neutral error messages
    - Run services only with minimal rights and as a separate user and in an isolated environment if possible
    - Enabling logging
    - Secure access points for remote access and remote users
    - If necessary, automate the installation of patches and updates
    - Secure configuration of software (e.g., deactivation of macros or JavaScript in Office applications) and browser.
    - Special protection of the Active Directory

4. Minimal assignment of authorizations (need-to-know principle, least privilege principle)
    - Review assigned authorizations regularly
    - Assign minimumrights for administrative activities
    - Assign minimum rights for file system and external data interfaces
    - Assign minimum rights for maintenance interfaces/accesses

- Restrict access to operating system configuration files
- Restrict access to the physical server (especially to avoid connection of unauthorized external disk drives)

5. Accounts and passwords
   - Use of strong uniform password policies for user passwords (e.g., password length, different passwords for all accounts, complexity, lock counter, change cycle, etc.) and use of 2-factor authentication (see chapters 3.2.1 – 3.2.3)
   - Protect all accounts with at least one password according to the password policy
   - Change all existing default passwords to passwords that comply with the password policy
   - Lock the local administrator account after several failed attempts of entering the password attempts
   - Deactivate or rename default user accounts
   - Deactivate local guest accounts
   - Disable the remote login of local user accounts
   - Disable standard, test, and anonymous accounts for all installed services/software components

6. Network Components
   - Restrict network settings (e.g., TCP/IP configuration), disable unused and insecure network protocols (e.g., Telnet, FTP, HTTP, SSL)
   - Disable unused network ports
   - Prevent a version downgrade during connection establishment ("handshake") (e.g., downgrading from TLS 1.3 to TLS 1.0)
   - Limit the number of connections made through a service to the minimum required
   - If necessary, activate of packet filters/firewall and ensure they have only the minimum required access

For common operating systems, detailed hardening guidelines are publicly available on the internet:
- CIS Benchmarks ("Center for Internet Security, Inc."): https://www.cisecurity.org/cis-benchmarks
- STIGs (Security Technical Implementation Guides): https://public.cyber.mil/stigs/
- Microsoft Security Guidance: https://blogs.technet.microsoft.com/secguide/

A large number of the hardening measures listed can be implemented by technical settings. For example, scripts can be used that automatically carry out the hardening on the systems. Group policy can also be used to enable automatic distribution of hardening settings in Windows-based infrastructures. When hardening existing systems, hardening can break functionality, so a data backup must be created and the hardening tested extensively.

A one-time system hardening without continuous maintenance of the safety level is ineffective. This can be achieved in particular through the following measures:

- BOM/DSL
- Change management
- Issue/patch management
- Release management

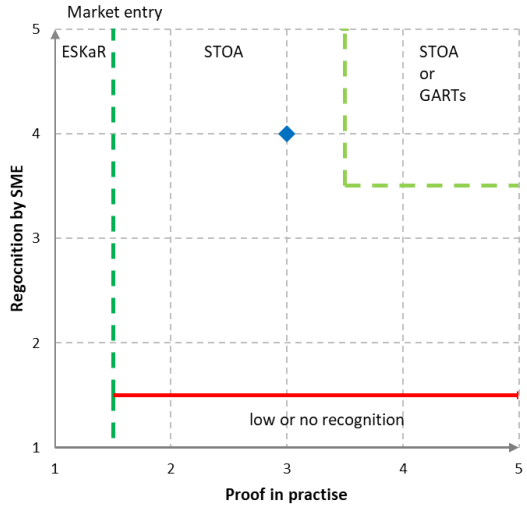
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.22 Endpoint Detection & Response Platform

The protection of end devices (e.g., PCs, laptops, smartphones or tablets) now requires much more than just an antivirus program. Modern solutions, such as endpoint detection and response (EDR) platforms, combine the latest protection technologies to stop all types of cyberattacks on client and server systems across operating systems and to identify the perpetrators. In contrast to conventional solutions, no specific prior knowledge, such as signatures or a first victim, is required.

Against which threat(s) of IT security is the measure used?

- Malware
- Exploitation
- Malicious scripts
- Hacker activities
- Misuse of administrative tools and tools designed for nefarious use

What action (procedures, facilities or modes of operation) is described in this section?

EDR platforms combine effective detection and prevention techniques to prevent the compromise of clients and servers beyond the boundaries of computers and operating systems, and even to expose active attackers on computer networks.

Lightweight agents provide the attack-relevant process telemetry data, use locally effective machine learning models (artificial intelligence), and holistically correlate and visualize tactics, techniques and procedures.

Using modern sensor architecture, signature-based threat detection is supplemented by a detection approach for anomaly detection. This means:

- Detection of known malware via signature-based protection components (more secure, saves computing time)
- Signature-free detection and active blocking of malicious code, ideally through supervised machine learning models (preferably local runtime)
- Audit and record program activity across process chains and optionally block malicious behavior
- Protection against exploitation of vulnerabilities within legitimate applications (exploits and memory manipulation)
- Ideally, data from different sources should be normalized and detections correlated, and the technique and tactics (including tools used such as malware, Trojans, PowerShell scripting and the attacker's goal (exfiltration of data, backdoor setup, lateral movement within the organization, privilege escalation, etc.)

- Optionally, threat intelligence can show who the suspected actor/adversary is (cybercrime or nation-state-motivated attack) and what goals and industries the attackers are pursuing.

EDR platforms address the entire lifecycle of an attack attempt. This is the only way to draw conclusions about the actors and their motivations, which are ideally contextually complemented by up-to-date threat information. In addition, system telemetry data can be checked by external experts for harmful indications.Along with detecting security-related events, EDR solutions provide options for manual and automated responses to these threats, such as automatic isolation of the device or deactivation of user accounts. Also, there are features to support incident response investigations, such as remote access capabilities or the provision of additional data with the provision of triage packages.

Furthermore, it must be noted that the following points in particular should be taken into account for the holistic protection of end devices:

- Roles/permissions (keyword: admin rights)
- Update mechanisms (operating system and software)
- Restrictions/control of installed software (application control)
- Encryption of the end devices
- Regulations/guidelines for permitted use (private use, use in external networks, travel, use of data carriers, storage of data, backup, etc.); especially if the user has admin rights (device control)
- Use of authentication methods (username/password, PIN, biometrics, etc.)

The current market trend is towards further development of extended detection and response (XDR) solutions. The combinations range from patch management, device management, backup tools, and encryption to network-based detection.

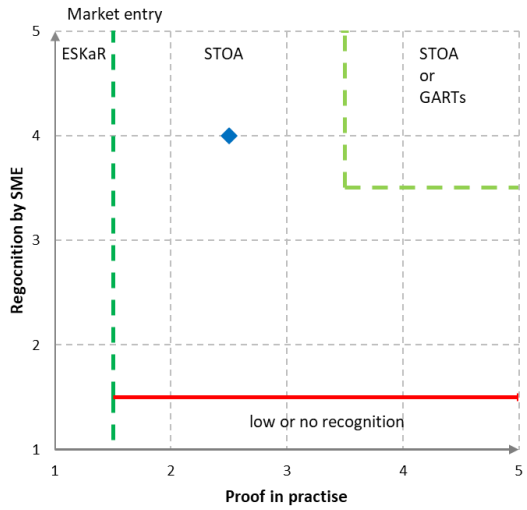
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.23 Web isolation of Internet usage

Web isolation separates the user's workstation from the browser sessions and enables secure Internet use without restrictions on content or functions. Browser-based cyber attacks, data leakage/loss and the associated productivity restrictions and image damage are effectively prevented.

Against which threat(s) of IT security is the measure used?

Infection of the workstation computer, for example by

- Browser vulnerabilities, drive-by downloads, infectious websites
- Ransomware, APT, Trojans, Viruses, Worms
- Zero-day exploits
- malicious links in emails

and thus, the spread of malware in the mission-critical network.

What action (procedures, facilities or modes of operation) is described in this section?

The isolation of browser sessions can be done in several ways. The decisive factors here are the architecture used and its security mechanisms. Examples are the so-called "remote-controlled" browser environments or multi-layered local browser isolations.

A simple isolation of the browser environment (e.g. via simple virtualization based on Hyper-V or so-called browser sandboxing) does not offer a sufficiently high level of protection against the aforementioned threats, as it does not have a secure hardened operating system in which the browser runs by default; does not use additional secured network segmentation; does not allow secure copy & paste or does not use additional security functions such as data locks. Therefore, this method is not suitable for defending against the threats.

Remote controlled browser environments based on ReCoBS

The Remote-Controlled Browser System (ReCoBS) separates Internet use from the user's device on a physical level. Each browser session is executed outside the sensitive network area in a specially sealed environment within a specially hardened system on separate hardware in a separate network segment (DMZ).

The browser is remotely controlled from the workstation via a video stream on the remote system via a technically secured communication channel. The majority of attacks targeting Windows-based vulnerabilities are already successfully mitigated in the hardened Linux environment. Other security mechanisms and zones in the overall architecture provide reliable protection against attacks even if the browser has been compromised. The physical separation of the workstation and browser system also provides protection against hardware-related attacks (Spectre, Meltdown, ZombieLoad or vulnerabilities in the hypervisor).

At regular intervals (once a day according to the standard), the remote system should be restored to its original state via a system image so that any malicious code is effectively removed. It is important to ensure that the system image is kept in integrity.

The user's workstation does not need direct access to the Internet at any time and is therefore additionally protected, e.g. against the reloading of malicious code by infectious documents that have reached the computer by other means - such as by e-mail or USB stick.

Since the ReCoBS architecture means that common standard functions of the browser are executed on the remote system due to the principle, additional developments are necessary for user acceptance so that the remote-controlled browser differs insignificantly from local browser use and all the usual functions such as personal bookmarks, copy & paste, printing or downloads and uploads are offered in principle.

For the optional transfer of files (browser download/upload) between the remote system and the workstation, additional checking mechanisms must be provided that move suspicious files to quarantine and notify administrators. An example of such a check mechanism is virus protection in the data lock.

In addition, central management of the overall solution is recommended, so that, for example, an existing directory service can be coupled and used to manage user roles.

Web isolation based on the local virtualization of the browser application

Another approach to web isolation is based on the local encapsulation of the browser application through secure virtualization in combination with a rights-limited Windows user account, hardened guest operating system, and Internet/intranet separation through a separate VPN tunnel to the Internet gateway. This excludes direct access from the browser session to the PC hardware.

One advantage of local browser isolation is the possibility of stand-alone use on mobile workstations. However, the lack of physical separation between the sensitive workstation and the browser system could make it possible to exploit local security gaps in the processor hardware or software to break into the end device via an exploit package that encompasses all layers of protection.

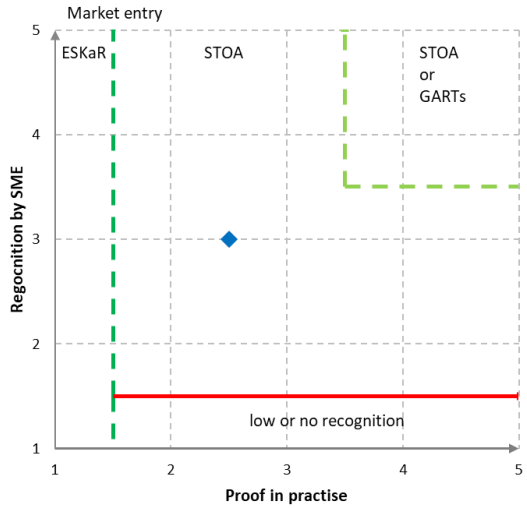
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.24 Intrusion Detection and Evaluation (SIEM)

So-called Security Information and Event Management Systems (SIEM for short) are used to evaluate anomalies and detect attacks on the company infrastructure. They make it possible to identify security-critical events of the IT infrastructure in real time and to carry out appropriate measures (partly automatically).

Against which threat(s) of IT security is the measure used?

SIEM can help against the following threats:

- Attack activities by external parties (hacker attacks)
- Threats from insiders (e.g. unauthorized access to data from other departments, computer sabotage)
- Compliance violations

What action (procedures, facilities or modes of operation) is described in this section?

A SIEM centrally collects log and event data from devices, network components, applications and security systems. For example, the following data sources can be mapped in the SIEM:

- Log files from operating systems
- Firewall events of network firewalls
- Alarms from Intrusion Detection & Prevention Systems (IDS/IPS)
- Intelligent network sensors / network monitoring systems with information about found assets/devices, vulnerabilities, compliance violations or anomalous network behavior
- Directory services Authentication services (such as single sign-on systems)
- Endpoint Detection & Response Systems (EDR/XDR)
- Indicators for the identification of attackers and attacks such as IP addresses, hashes, hostnames, etc. (threat intelligence feeds) as well as e.g. contextual information on attackers for enrichment

The security team in the company has the opportunity to obtain a holistic picture of the processes in its IT solution/infrastructure in real time through targeted aggregation and analysis of security-relevant event and system logs. This makes attacks, unusual patterns and dangerous processes visible. Based on the insights gained, companies are able to react quickly and accurately to acute threats. Based on the available data, the patterns can be analyzed in the aftermath of an attack (forensics) and the existing measures can be improved.

Modern SIEM tools include robust and out-of-the-box detection rules that can be adapted to new threat cases. The operation of a SIEM solution requires the integration of suitable sources but also the provision of significant system resources (e.g. graph databases, data lakes and servers for operation and management). At the same time, a significant bandwidth utilization is achieved through the continuous exchange of data. The associated administrative complexity and the acquisition and operating costs are quite high, which is why classic SIEM solutions are usually used in large and very large companies.

Cloud-based and third-party managed solutions such as SIEMaaS (SIEM as a Service) are a contemporary alternative with easily calculable costs. They also enable the technology to be used in small and medium-sized companies. A modern endpoint detection & response platform (EDR/XDR) with its interfaces to security orchestration, automation and response (SOAR), user and entity behavior analytics (UEBA), network security products such as next-generation firewalls and integrated threat intelligence can also be a sensible alternative.

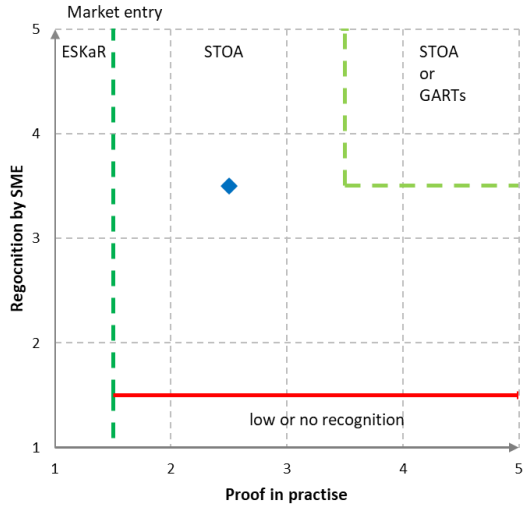
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.2.25 Confidential data processing in the cloud

Privileged access by administrators to data during processing is traditionally only secured against abuse of the privilege with organizational or reactive measures. With the help of confidential computing, this data is tamper-proof and preventively protected against unauthorized access. This is important for applications in the field of cloud computing. Confidential data processing meets the need for protection when cloud services are used for critical infrastructures or for sensitive data processing operations, such as in medicine, industry or regulated areas.

Against which threat(s) of IT security is the measure used?

Cloud administrators are responsible for the trouble-free operation of their systems. In order to be able to fulfill this task, they are granted numerous privileges. For example, they can adjust the system configuration and read out memory contents. This means that data can be compromised on its way to the cloud, in cloud storage and during processing in the cloud not only by attacks by third parties, but also by unlawful employees of cloud service providers.

What action (procedures, facilities or modes of operation) is described in this section?

Previous approaches to data backup have been based on data at rest (storage) and data in transit (network). Confidential computing focuses on the protection of data during processing. This is an area or capsule (virtual machine, application, or function) shielded from the outside world, in which the entire data processing takes place in an unencrypted state. This shielding can be implemented either directly on the processor chip of the servers (hardware-based trusted execution environment) and/or across several servers at once. In order for the data to be processed, the required key must be available inside the capsule. If an attacker were to try to gain access to the encapsulated area, the unencrypted data processed there would inevitably be deleted as a precautionary measure. To achieve increased security, the capsules can be sealed by independent auditors after prior verification using known cryptographic secrets.

In the case of data processing systems equipped with the measures summarized under the generic term "confidential computing", a single administrator cannot gain access to the data processed in the server. Only through a malicious coalition of several independent parties (e.g. system administrators together with their independent auditors) can the technical measures be overridden. This reduces the likelihood of improper access by several orders of magnitude.

Confidential data processing

- allows data to be processed in central infrastructures without exposing them to the possibility of knowledge by the operators of this central infrastructure,
- Provides users with more control and, depending on the audit, transparency

- offers new degrees of freedom, because new applications are conceivable that cannot be implemented in a legally compliant manner under conventional data protection and security considerations.

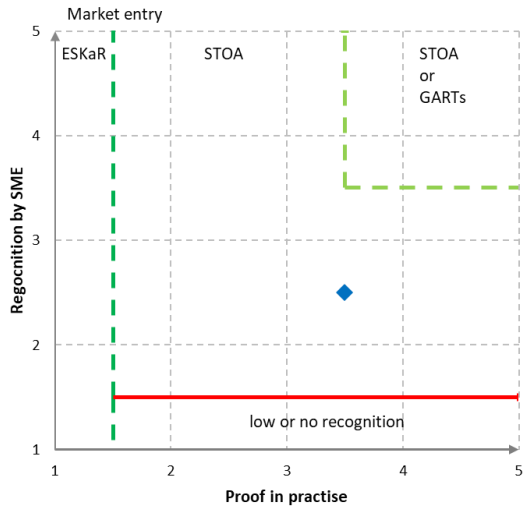
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.26 Sandboxing for malicious code analysis

Sandbox technology is used to execute potentially dangerous files in an isolated environment and check for malicious behavior. Running in a separate environment prevents possible infection.

Against which threat(s) of IT security is the measure used?

- Hacker activities in the sense of
- Malware (viruses, Trojans, etc.)
- Phishing

What action (procedures, facilities or modes of operation) is described in this section?

The use of the sandboxing method for automated malware analysis is common in two use cases.

Perimeter Sandboxing

In the context of perimeter sandboxing, file attachments (such as documents from the active environment, but also embedded content such as scripts) from e-mails are usually executed automatically. The sandbox analysis at the email gateway usually generates a latency in the user's access to the examined file attachment that is in the range of a few seconds to minutes.

Sandboxes can also be used at the web gateway (next-generation firewall or proxy), e.g. to check downloaded programs. Here, too, a delay is caused until the file is delivered to the user. In addition, its use also influences the behavior of browsers and web-based software. Therefore, in addition to the classic functionality of sandboxing (first check, then delayed delivery), delivery of the file to the end device with parallel verification is also practiced. If malicious code is identified in the latter procedure, subsequent

measures are taken. These include network isolation, blocking "command and control" addresses that were determined during sandbox execution.

Sandbox for forensic examination of files in the context of detection or investigation

By connecting sandboxes to next-generation antivirus products (machine learning-based antivirus) and EDR solutions (endpoint detection and response), files with a malicious prognosis or from detected and actively prevented attack chains can be safely executed outside the active environment. The execution then allows the extraction of further relevant indicators (files/hashes, URLs, IP addresses, registry activity, etc.), which gives more context to a case under investigation and even the attribution of a suspected attacker.

Since sandbox solutions have a fairly high degree of distribution, attackers repeatedly try to prevent detection in a sandbox. For example, when executing their malicious code, they try to determine whether it is a virtualized runtime environment - as is common in sandboxes - or an active environment with certain programs/processes and other specific characteristics. The malicious code will then usually behave harmlessly to avoid detection. However, this behavior can also be detected in the sandbox and used to identify suspicious content (cat and mouse principle).

The exploitation of so-called "day-0 exploits" / zero-day threats, i.e. vulnerabilities that are previously unknown to the public, can also lead to sandbox bypasses. It can also happen that the emulated runtime environment does not correspond to the victim system and thus the behavior when executed in the sandbox differs from that on the target system of an attack. It is therefore necessary to master these tactics, known as "sandbox evasion", for example by combining static and dynamic analysis.

Sandboxes continue to offer great benefits due to their high level of automation, therebymassively reducing the need for manual analysis of malicious code (so-called malware reverse engineering) by an expert.

There are a large number of open source and commercial sandboxes. These are offered as mostly cost-intensive hardware solutions, but also as publicly or privately provided cloud solutions. For some time now, sandbox technology has also been used in browsers to detect common types of attacks at an early stage.

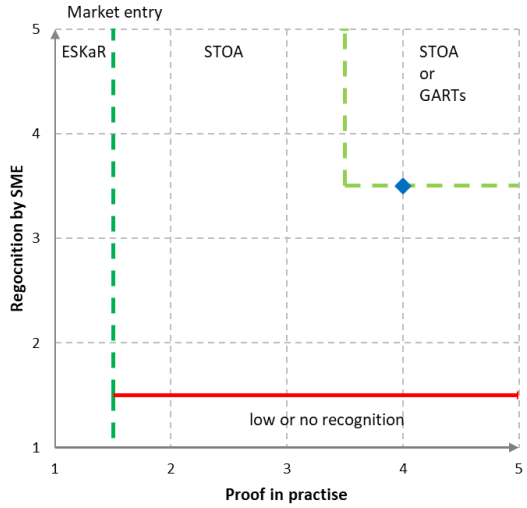
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.27 Cyber Threat Intelligence

Cyber threat intelligence is an important basic building block of modern defense strategies and provides indicators, reports and services to inform oneself about the current attack situation, to detect cyber attacks, to determine their presumed perpetrators and to derive countermeasures.

Cyber Threat Intelligence is divided into three areas of application:

- Tactical cyber threat intelligence includes malware analysis and the import of single, static, and behavioral threat indicators into defensive IT security solutions such as network, endpoint, and application security solutions to increase their effectiveness. Indicators obtained through cyber threat intelligence can play an important role in measures such as system patching.
- Operational cyber threat intelligence is used to improve knowledge about an attacker, their capabilities, infrastructures and attack tactics, as well as techniques and procedures (TTPs). This information can be used to implement much more targeted cybersecurity measures such as incident analysis, incident response and proactive threat hunting. This improves the performance of cybersecurity personnel (e.g. from the Security Operation Center or CERT) such as threat hunting experts, vulnerability managers, incident response analysts and insider threat defense experts.
- Strategic threat intelligence enables a better understanding of the current threat situation (threat assessment), the derivation of trends and the motivation of individual attacker groups. It supports strategic business decisions to improve cybersecurity.

Against which threat(s) of IT security is the measure used?

Cyber Threat Intelligence provides information about all types of current and potential cyber threats and helps to defend against them.

What action (procedures, facilities or modes of operation) is described in this section?

Tactical Cyber Threat Intelligence (TM)

Integration of threat indicators (feeds) into existing endpoint and network detection & response systems, system management solutions, firewalls, IDS/IPS and SIEM/SOAR solutions with the aim of identifying real attacks and supporting analyses (including retro hunting), as well as preventing compromises. For optimal effectiveness, the indicators should be able to be used automatically for the detection and prevention of cyberattacks. The sources for threat intelligence indicators may allow conclusions to be drawn about their reliability and are differentiated into:

- Open-Source Intelligence (OSINT),
- Events from private honeypot systems,

- Insights from attack analytics from real customer environments, or the
- Investigative work by intelligence-trained experts

Operational Cyber Threat Intelligence (TM/OM)

Organizations that operate a Security Operation Center (SOC) and may have their own Computer Emergency Response Team (CERT) use threat intelligence operationally to continuously inform themselves about the actors and their TTPs. In addition to access to indicators, comprehensive threat intelligence platforms also offer different report formats (short news, situation reports, attacker profiles) as well as access to malware databases, sandbox technology for automated malware analysis and malware reverse engineering. Furthermore, there should be the possibility to access analysts directly to the provider and to submit research requests (RFIs).

Strategic Threat Intelligence (OM)

Both the areas of information security and the overall security of large companies use threat intelligence to create as complete a picture of the situation as possible. The focus is on the geopolitical situation as well as industry-specific and global trends in the threat landscape. Access to a dedicated employee at the provider virtually expands your own team and ensures that direct access to its data pool is provided, as well as customer-specific investigative work is optimally performed.

Providers of modern IT security solutions deliver, integrate, and automate threat intelligence so that threat indicators and relevant attack telemetry are meaningfully linked, preventive measures are automated, and attacker attribution is enabled without the need for additional systems and even human resources.

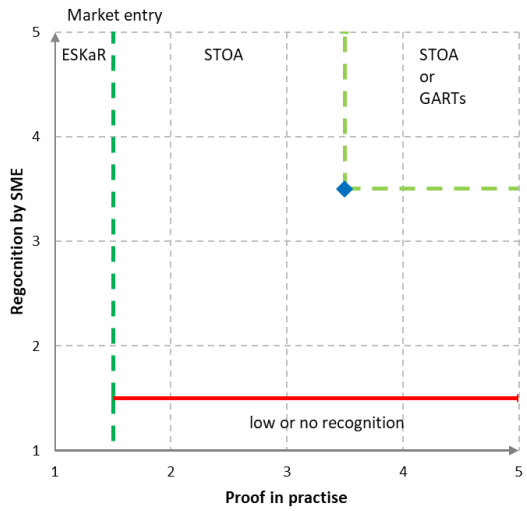
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.28 Securing administrative IT systems

Administrative IT systems are clients and servers that manage and monitor other IT systems using management applications. Compared to standard workstations, administrative IT systems are usually located in dedicated network segments in which additional network protocols are used and from which the administrative interfaces of systems can be reached. Due to this special use of administrative IT systems, these systems pose a risk with great potential for damage (e.g. access by unauthorized persons). Therefore, regulations and measures appropriate to the risk must be taken to protect against unauthorized access and to maintain secure IT system administration – in particular with regard to the protection of the privileged accounts used on the systems and the necessary connections.

Requirements for administrative IT systems

Administrative IT systems must be secured in accordance with the system hardening measure (see Chapter 3.2.21).

Regulations and measures must be defined for the use and handling of administrative IT systems as well as for their protection. Before granting access to a user, the user must first accept these rules and undertake to comply with them. A violation of the defined regulations must be clarified and have consequences.

Access to administrative IT systems may only be granted to qualified employees or approved for them. Administrative IT systems are to be used exclusively for the administration of systems and must be secured with hardening measures and strong authentication methods according to their protection requirements. Their protection requirements must be identified and protected by appropriate measures.

Access to administrative IT systems may only be possible for authorized administrators after successful authentication via a secure login procedure. This requires a suitable authentication procedure for the identification of the user, which corresponds to the protection requirements of the system to be administered (e.g. multi-factor authentication, see Chapter 3.2.3). When entering access data such as passwords or PINs, this data must not be displayed by the system. When logging on to administrative IT systems over the network, the data used to authenticate the user must be transmitted in encrypted form using secure protocols. Inactive remote sessions must be automatically logged out/terminated after a defined period of time.

If the administration requires a connection to a network segment with systems with a high or very high protection requirement (e.g. to a network segment with SCADA/ICS systems), the administration or the network connection must be made via a jump server/proxy server in a DMZ between these network segments.

There must be minimum standards for passwords for administrative IT systems. These systems must also be integrated into state-of-the-art authorization systems, whereby the connection and the authorization system itself must be particularly secured/hardened. Furthermore, personalized accounts must be used, which can be uniquely assigned to a person. Do not use standard users and passwords.

It must be ensured that only permitted software components, programs and scripts are executed on administrative IT systems. If an addition of software components, programs or scripts is necessary, approval must be made as part of a corresponding process before its use and the use must be documented and monitored.

On administrative IT systems, the login processes and activities of the administrators must be logged so that it can be traced which activities were carried out by which persons (accounts). To ensure the traceability of the activities performed, administrators must not modify or delete the log and audit logs of their own activities with their accounts. For critical administrative activities, the principle of multiple eyes should be applied.

The following measures for appropriate protection are recommended as examples for the establishment:

- ISO/IEC 27002: The standard contains recommendations for the implementation of the measures required in ISO/IEC 27001 Annex A for access control and for the operational security of systems, which also apply to administrative IT systems. If certification in accordance with ISO/IEC 27001 is sought, these measures must be implemented within the scope of the

ISMS. Implementation instructions for this measure can be found primarily in Sections 9 "Access Control" and 12 "Operational Security".

- BSI IT-Grundschutz Compendium: The BSI IT-Grundschutz Compendium describes numerous measures for the protection of systems in its modules SYS.1, SYS.2 and IND.1. These building blocks are also relevant and applicable to administrative IT systems. The implementation of the requirements listed for a high or very high need for protection in the building blocks is recommended.
- BDEW Whitepaper: Requirements for Secure Control and Telecommunication Systems. The BDEW Whitepaper contains supporting information for securing administrative IT systems, such as the use of secure protocols and jump servers for (remote) access as well as the placement of systems in dedicated network zones.

The requirements for operational security and access protection of administrative IT systems must be reviewed periodically (at least annually) for completeness and adequacy and updated in accordance with an access or access control policy.

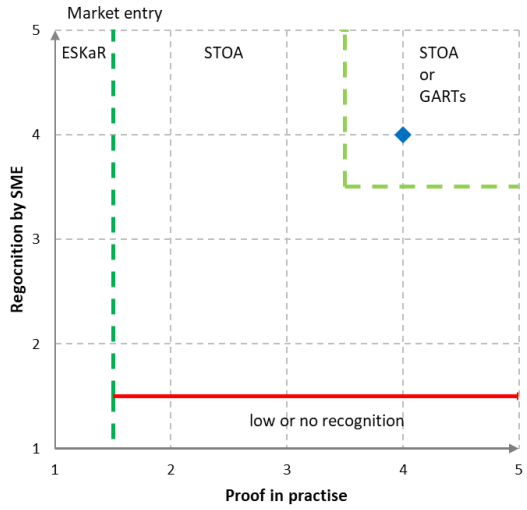
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.29 Directory Service Monitoring and Identity-Based Segmentation

A large portion of serious cyberattacks by state-motivated actors and cybercriminals involve directory services and user accounts. These include complex attacks via the supply chain, resulting in espionage and sabotage. It is therefore essential for companies and organizations to reduce their attack surface, identify and avoid unnecessary risks at an early stage. Attack attempts and unusual access should be detected as they arise and contained in real time - even if endpoint protection and IPS systems fail, and the attacker is using valid access credentials that were stolen.

Against which threat(s) of IT security is the measure used?

- Attacks that exploit captured/'leaked' usernames and passwords (e.g., credentials obtained from a dark web data breach) and do not involve any malware component
- Exploitation of vulnerabilities in directory services (insufficiently protected service accounts)

- Spread and movement of an attacker in the organization (lateral movement)
- Compromise and abuse of privileged accounts and elevation of privilege

What action (procedures, facilities or modes of operation) is described in this section?

Assessment/audit of directory services: Modern protection solutions combine the hygiene status of directory services such as Microsoft Active Directory, Microsoft Entra ID and other "Identity as a Service" solutions to prophylactically treat vulnerabilities and create risk profiles. These include:

- Detection of poorly protected service accounts
- Identification of hidden privileges that go beyond group membership, such as delegation or abuse of privileged SIDs,
- Detection of attack paths to privileged accounts that are typically only uncovered in the course of complex audits (e.g., via tools such as SharpHound/Bloodhound)
- Threat monitoring with darknet monitoring

Real-time monitoring and analysis of all relevant authentication traffic, both locally, such as Kerberos, NTLM, LDAP, RDP, RPC, etc., as well as from cloud-based IDaaS and federation services, to detect attack attempts or the use of so-called reconnaissance tools and to provide the Security Operation Center with comprehensive and enriched information. Integration with cloud-based services can also capture geo-location-related anomalies and detect deviations from normal usage.

Based on the individual protection needs of the respective organization, an identity-related set of rules can then be implemented, taking into account the risk profiles, which, for example, prevent user accounts with poor risk scores from accessing critical applications or local critical resources. It should also be possible to react automatically to unusual user behavior and demand measures, such as requesting an additional authentication factor (MFA). This enables protection that combines the focus of specialized classic solutions such as privileged access management (PAM) with that of user and entity behavior analytics(UEBA) and at the same time is easy to apply in practice, e.g., by deploying a sensor application to the directory servers, as well as API-based integration into federation services and cloud directory services. The application of machine learning models significantly reduces the effort here. [18]

The consistent segmentation of identities within identity providers – for example, in the widely used directory service Microsoft Active Directory – is an effective measure to prevent lateral movement across divisional boundaries. All identities and their associated resources (e.g., user groups or computer accounts) are organized according to the Active Directory logical model and are thus strictly separated from each other by logical layers. In the event of a compromise, an attacker's access to the identities within a single layer cannot be ruled out, but segmentation prevents it from spreading to other layers. This keeps unaffected areas protected and significantly reduces the risk of the entire identity system being compromised. This approach is conceptually based on network segmentation; however, the demarcation is not physical, but logical within the identity store. In addition, appropriate guidelines must be defined and enforced to prevent a transition between the shifts. The implementation of this principle is often known in practice under the terms "tier model" or in extended form as "plane model" and Microsoft also refers to it as the "Enterprise access model" (EAM).

Note: All of the above-mentioned sub-areas represent important building blocks and actively contribute to the implementation of a zero trust framework. Access rights can be effectively implemented, even without or in addition to network-side restrictions (firewalls). The data protection aspect must also be taken into account here, especially when it comes to the analysis of user activities.

What protection goals are covered by the measure?

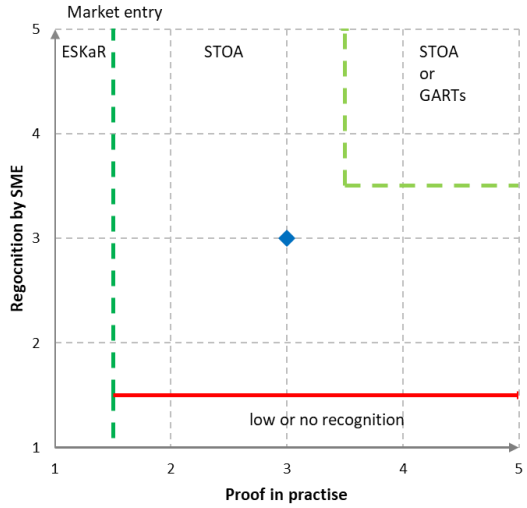
☐ Availability

☒ Integrity

☒ Confidentiality

[18] See also sections 3.2.1 Authentication, 3.2.3 Multifactor authentication and 3.2.24 Security Information and Event Management (SIEM)

Classification of the measure



3.2.30 Network segmentation and separation

Splitting networks through network segmentation and separation is an effective measure to reduce threats to the availability, confidentiality, and integrity of networks and the systems they contain. Segmentation and separation also support hedging as part of the defense-in-depth approach.

Network segmentation is the process of dividing a network into several segments, each of which acts as its own subnetwork. Communication between these segments is limited by defined zone boundaries (boundary protections) with checks and monitoring of the network connections. Zone boundaries between networks, such as information technology (IT) and operational technology (OT) networks, reduce many risks , such as malware threats. Zone separation, or segmentation, restricts access to systems, data, and applications, and limits communication between networks. This approach protects segments in the network from attacks from other segments that have already been affected.

Against which threat(s) of IT security is the measure used?

- Network lateral movement
- Unhindered spread of malware in networks
- Insider threats, e.g., unauthorized access to systems from other departments or locations
- Illicit or malicious traffic can be more difficult to identify due to network sizes and data volumes.
- Exploitation of access options to networked IT systems
- Loss of availability, integrity, and confidentiality of a large number of systems when they operate on a flat network and are compromised
- Loss of availability of critical systems in the network due to attacks on non-critical systems that have fewer security measures

What action (procedures, facilities or modes of operation) is described in this section?

For network segmentation, a network must be divided into several so-called network zones (or subnetworks), whereby a network zone forms a logical group of devices, applications, and systems with common security requirements (same protection requirements). The use of critical and non-critical systems in a network zone is not permitted, even if they can be grouped thematically or have a high level of communication with each other.

The separation of the network zones can be logical (e.g., by VLANs) and/or physical (e.g., by a dedicated switch infrastructure for the zone). The decision as to whether physical separation is required must be based on regulatory requirements or a risk-based approach.

All data traffic between different network zones must take place via defined and appropriate zone transitions and must be released in advance. In the case of zone transitions, restriction, control and

monitoring of network traffic must be implemented with, .for example, firewalls/IPS/ACL. Mechanisms for detecting security-relevant events in network traffic (e.g., firewall/IPS, logging on network devices and sensors/IDS) must be implemented on a risk-based basis and can be analyzed and evaluated, for example, by a SIEM.

A whitelisting approach should be used for zone transitions. All traffic is blocked by default, and only defined traffic is allowed (deny by default, allow by exception). Network connections between systems in different network zones (especially with different protection requirements) must be kept to the necessary minimum, and, if needed, separate transfer interfaces must be implemented in separate zones (e.g., DMZ).

For network segmentation, an architecture based on the defense-in-depth principle must be planned and implemented. For this purpose, zones for external or untrusted networks (e.g., Internet or visitor WLANs), zones for DMZ systems (e.g., proxy systems or jump servers for external access) and zones for internal systems (e.g., servers, clients, printers, etc.) must be provided. Separate zones must be provided for systems that are supposed to be isolated (e.g., systems without security updates/maintenance). Industrial networks, iSCSI/storage networks and IT networks must always be physically separated from each other.

All network traffic with third-party networks (e.g., internet for downloading updates, remote access from external service providers) must be terminated by proxies, jump servers, VDI environments, etc., in a DMZ and have its network traffic monitored. Direct communication from third-party networks to internal network zones is not permitted.

Depending on the need for protection and criticality, the necessary protection/hardening measures must be defined and implemented for the individual zones.

Apart from active network devices, each system should be located in only one logical zone. Routing of network traffic on hosts/VMs between network adapters or the placement of systems in several networks (multihoming) must be avoided as a matter of principle and may only be carried out in released and documented situations after a risk analysis has been conducted and with necessary protective measures and zone transitions in order not to create uncontrolled transitions between zones. Furthermore, split tunneling for remote devices connecting to corporate systems should be prevented. Split tunneling allows a remote person or device to connect to a secure network while communicating with a resource on an external/insecure network via another connection. Exceptions in which split tunneling is intended, such as for video conferencing solutions that are allowed to access central cloud systems without a tunnel, must be defined.

Dedicated networks must be provided for administrative systems, which may only be used for administration. Administrative access to out-of-band networks on management interfaces of servers, network devices or KVM systems should only beallowed from networks for administrative systems.

In conjunction with the zero trust principle, so-called micro-segmentation is increasingly being used. Here, the attack surface is reduced by dividing the network into segments that are needed to run an application (e.g., virtual machines, containers, services).

The following standards are recommended for implementing this measure:

- **BSI IT-Grundschutz Compendium**
  In the NET.1.1 module "Network Architecture and Design", the BSI IT-Grundschutz Compendium describes requirements for the specification, planning, implementation and testing of network segmentations as well as for securing the network communication connections that take place via the zones.
- **ISO/IEC 27002:2022**
  The ISO/IEC 27002 standard contains recommendations for implementing measures in the area of network security (Control 8.20), security of network services (Control 8.21) and the separation of networks (Control 8.22).
- **IEC 62443-3-3 The IEC 62443-3-3 standard** contains specifications for network segmentation and for the control of network zone transitions in industrial communication networks in FR 5 "Restricted Data Flow".

Audits must be carried out periodically and on an ad hoc basis to check whether existing networks and network segments comply with the defined specifications and regulations, as well as the current documentation.

The documented guidelines, procedures and control measures for network separation that are essential for operation must be periodically reviewed for completeness, effectiveness, appropriateness and also for changed framework conditions and updated, if necessary.

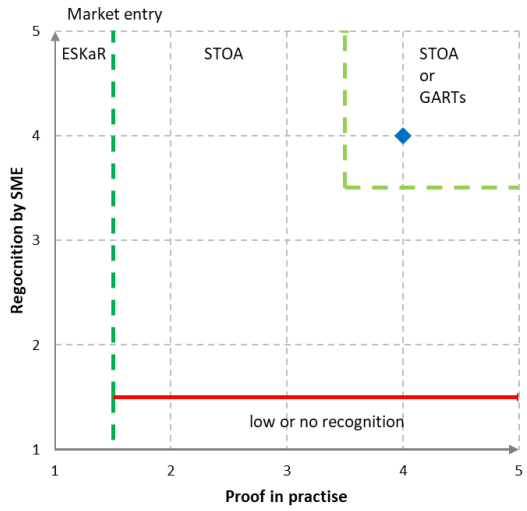
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.31 Cloud Security Platform

A cloud security platform is a technical measure that manages the risks and threats in provisioning cloud resources. A cloud-native application protection platform (CNAPP)encompasses individual areas such as container scanning, cloud workload protection (CWP/CWPP), cloud security posture and compliance, and active workload security, enabling a holistic view of cloud security. Cloud security platforms can reduce operational overhead and enable faster, more accurate detection, response, and remediation of security incidents by automatically linking otherwise siloed security information.

Against which threat(s) of IT security is the measure used?

- Misconfigurations in cloud infrastructure components and their configuration are continuously monitored. Settings and properties that do not comply with recognized security best practices, such as CIS benchmarks or compliance frameworks like ISO/IEC 27001 and SOC2, as well as their own defined requirements, are evaluated, and those responsible are alerted accordingly. This also includes the analysis of infrastructure as Ccode (IaC). Some examples of IoC would be Terraform HCL, Cloud Formation, CDK, Docker Files or Kubernetes Manifests.
- Vulnerabilities (Vulnerability Management): Vulnerabilities in applications in all phases of the development lifecycle from development, testing/staging to production, with prioritization by detecting active packages and images through runtime monitoring
- Malicious intrusions into cloud provider accounts by unauthorized third parties and attacks, detection by user and entity behavior analytics (UEBA). This is achieved through continuous

analysis of cloud audit logs, Kubernetes activity logs of known and previously unknown attack activity - without any concrete prior knowledge of the attack vector (vulnerability, pattern, IoC).
- Misconfiguration and monitoring of the security properties of serverless functions, containers, container orchestration, and virtual machines – before and during execution (CWPP)
- Unnecessarily high authorizations (CIEM) due to the visualization and resolution of complex authorization chains of accounts and resources

What action (procedures, facilities or modes of operation) is described in this section?

A cloud security platform covers the entire lifecycle of cloud applications, from application development to provisioning and production runtime. This makes it possible to discover vulnerabilities and misconfigurations before they are up and running, and to help developers and DevOps teams avoid unnecessary and unacceptable risks. At the same time, compliance with the compliance frameworks relevant to the user is checked. The check can be carried out by integrating scanners within the software pipelines, and corresponding policy enforcements are also implemented at the execution level (e.g., Kubernetes admission controllers).

In production, sensors on the compute instances and Kubernetes worker nodes ensure continuous monitoring of the security-related workload and network connections in order to detect attack attempts or malicious activities at an early stage. Machine learning-based methods can relieve the security teams by largely eliminating the need to create and continuously adapt sets of rules and attacks can be detected even without specific prior knowledge (behavior, file hashes, IP addresses, etc.). These incidents are contextually enriched. This allows for better classification, evaluation, or prioritization. Sensors, in the form of agents on the respective host systems in the company's own data center, support hybrid architecture and cloud migration projects. Agentless measures provide protection in environments where an agent cannot be deployed. Requirements such as host intrusion detection, file integrity monitoring, malware scanning and the detection of secrets (such as SSH keys) or the detection of possible attack paths are not only important, basic functions, but they are also important measures for meeting compliance requirements.

A cloud security platform that is independent of the cloud infrastructure operator enables multi-cloud architectures to be secured. At the same time, the independence from cloud provider-specific tools prevents vendor lock-in, i.e., technological dependence on a specific cloud service provider. The seamless integration with existing workflows and tools (e.g., ticketing, alerting, etc.) enables interdisciplinary cooperation across teams and projects.

In summary, the recommended actions of a cloud security platform are at least:

- Audit of IaC before provisioning resources (compliance, misconfigurations (IaC / Code Security)
- Compliance audit and detection of cloud misconfigurations (CSPM) and Kubernetes (KSPM) resources against relevant compliance and recommended best practices frameworks
- Prioritized vulnerability analysis from development to runtime (vulnerability management)
- Visualization of possible attack paths, chaining of vulnerabilities, authorization keys and misconfigurations (CASM)
- Inventory of cloud infrastructure components
- Authorization verification (CIEM)
- Behavioral analysis and early detection of malicious activity within cloud Aacounts (UEBA)
- Immediate detection of malicious activity through sensors within active workloads, including malware detection and file integrity monitoring (CWPP)

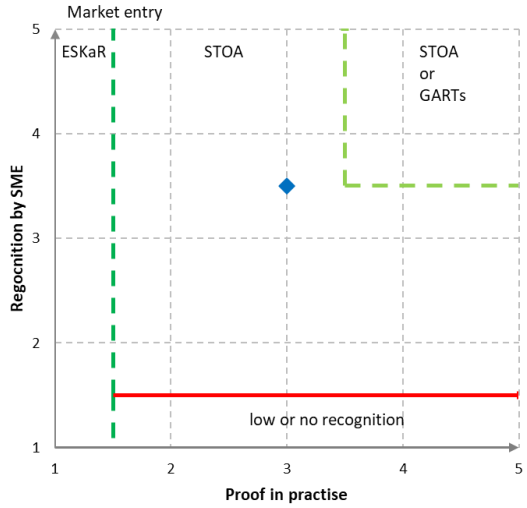
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.32 Tokenization

Tokenization is a method of data pseudonymization that can be used as an alternative to encryption. Here, a randomly generated replacement value is assigned to an original value, and both values are stored (encrypted) as a link in a mapping table in order to restore the original value if necessary.

Against which threat(s) of IT security is the measure used?

- Breach ofconfidentiality of (highly) sensitive data, such as customer data, employee data, or data from production or development (e.g., against administrators and software developers, who are not allowed to have access to production data)
- According to the EU General Data Protection Regulation (GDPR), pseudonymization minimizes the risk of personal data falling into the wrong hands. This applies in particular to unauthorized access or use. Tokenization as a specific pseudonymization method protects highly sensitive data in cloud-based environments and during transmission.

What action (procedures, facilities or modes of operation) is described in this section?

Tokenization describes a process for data pseudonymization, which is characterized by the ability to preserve the format of the target values. It is therefore particularly suitable for generating test data or protecting data in cloud-based applications (see also Chapter 3.2.12, Protection of files stored in the cloud).

Most of the time, tokenization is complementary to encryption, as it is not superior to encryption per se, but still offers some advantages:

1. Format preservation: The generated surrogate value must conform to a predefined format so that field validations continue to be successful, e.g., for email addresses or bank details.
2. Statistical distribution: The statistical distribution of the generated substitute values corresponds to that of the original values, which can be advantageous, for example, in statistical surveys (think of postal codes, blood values, etc.). However, a tokenization tool should provide the ability to configure this behavior for maximum flexibility.
3. Mathematical independence: Unlike algorithm-based encryption, a mathematical calculation cannot be used to derive the original value. Instead, the relationship between the original value and its tokenized value must be stored in a mapping table. As long as the token database remains confidential, tokenization is difficult to break. According to the recommendation of the European Data Protection Board, technical and organizational measures must be implemented to ensure that the assignment of tokens to original data is only possible by authorized parties. Therefore, it is recommended to use an HSM to encrypt the original values in the mapping table.

However, tokenization also offers disadvantages compared to data encryption:

1. To maintain performance during processing, appropriate computing power is required. For large amounts of data, algorithm-based encryption is often the better choice.
2. A so-called token vault must be created, in which the original values are stored securely and encrypted alongside the replacement values. This can result in larger amounts of data that require appropriate storage capacities.
3. The token space is finite: the stricter the requirements for the format of the substitute values, the smaller the number of substitute values that can be generated.
4. Another aspect is that pseudonymized data is still considered personal if additional information is available for repatriation. Therefore, this information must be specially protected and kept separate.

Despite all its advantages, tokenization is not an end in itself: The focus is on the protection of data, which is why software solutions for tokenization should have the following convenience features:

1. Independent solution: No changes are required to the target applications where the tokenized data resides.
2. Possibility to tokenize individual values in files, databases, and web applications, in addition to the basic functionality that provides tokens via modern interfaces.
3. Availability of complex token profiles, such as the Luhn algorithm for the correct generation of credit card numbers, or the ability to generate pronounceable strings as a surrogate value. Ability to selectively tokenize, so that fields can be protected or retained unaltered, depending on the sensitivity of the data and the level of protection required.

In accordance with Art. 25 GDPR, tokenization meets the requirements of data protection by design if it is combined with appropriate technical measures, e.g., by using cryptographic methods or by implementing a hardware security module (HSM). The effectiveness depends on the separation of the pseudonymization component from the data processing.

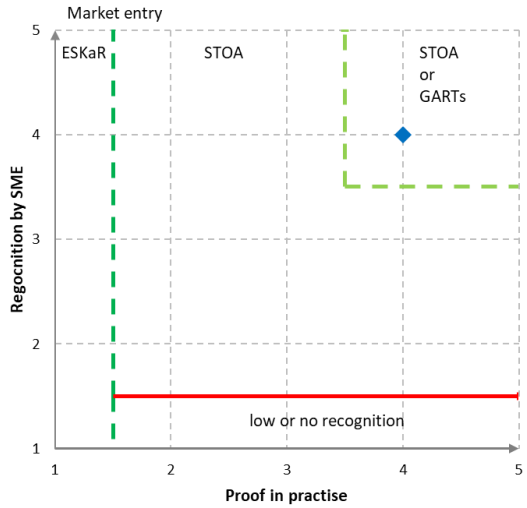
What protection goals are covered by the measure?

☐ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.33 VOIP encryption with SIPS/SRTP

Today's telecommunicationsuse IP-based networks as their foundation. The Session Initiation Protocol (SIP) is used to control connections (e.g., call establishment and disconnection, forwarding and changes in connection parameters) and signaling. The Real-time Transport Protocol (RTP) is used to transmit digitized audio and video. Both normally work unencrypted. They are therefore initially vulnerable to the threats of inspection, eavesdropping, manipulation and disruption of availability by unauthorized third parties. In addition, communication patterns can also be derived.

Against which threat(s) of IT security is the measure used?

- Listen to and record phone calls (even a small amount of voice data can be used to clone voices with AI)
- Faking false identities or unauthorized redirection of conversations through manipulation (caller ID spoofing)
- Injection of unauthorized voice data or silence
- Voice data overlaid with noise can be controlled by voice-controlled devices
- Establishing unauthorized connections
- Denial-of-Service Attacks

What action (procedures, facilities or modes of operation) is described in this section?

To encrypt the signaling, transport encryption based on SIP over TCP and TLS in combination with the SIPS URI scheme can be used. The Secure Real-time Transport Protocol (SRTP) is used for encrypted voice transmission.

The SRTP enables the encrypted transmission of voice data with any sensitive and personal content it may contain. The protocol provides confidentiality, integrity, and protection against replay attacks. It uses symmetric encryption based on the Advanced Encryption Standard in Counter Mode (AES-CM). Depending on the key exchange method, key lengths of up to 256 bits can be used. However, it should be noted that only the user data is encrypted. The header is merely authenticated. HMAC-SHA1 with 80 bits serves as a hashing method to ensure integrity.

The use of Security Descriptions for Media Streams (SDES) for key exchange only makes sense in combination with TLS-encrypted SIP signaling, as in this case the key exchange for SRTP takes place within the signaling in plain text and otherwise subsequent decryption would be possible.

Datagram Transport Layer Security (DTLS) is the UDP-based counterpart to TLS. It is therefore a transport encryption that builds on X.509 certificates to exchange the keys and algorithms for SRTP. However, the transmission of the user data does not take place via DTLS, but via SRTP. The symmetrical SRTP keys are exchanged directly via the media path and not within the signaling. The endpoints transmit a fingerprint of the certificates in SIP signaling as authentication. Only the media endpoints have access to the keys.

The encryption of signaling via SIP-TLS basically works "hop by hop". This means that encryption is initially only ensured until the next SIP proxy. This next SIP proxy can decrypt the data and make a forwarding decision based on the signaling in plain text. SIP-TLS based on the so-called SIPS URI scheme goes a little further. Encryption up to the target domain is used and should therefore be used preferably.

In principle, authentication can be carried out either purely server-based (via SIP proxy or SBC) or mutually between client and server (so-called mutual TLS). Mutual authentication should be preferred.
For SIP-TLS, only version TLS 1.3 should be used. The corresponding algorithms and hashing methods should be selected according to BSI recommendation TR-02102[19] . DTLS in connection with SRTP should also only use DTLS 1.3. Since personal data is transmitted, forward secrecy should be used to avoid subsequent decryption.

[19] Technical Guideline TR-02102-2: Use of Transport Layer Security (TLS)

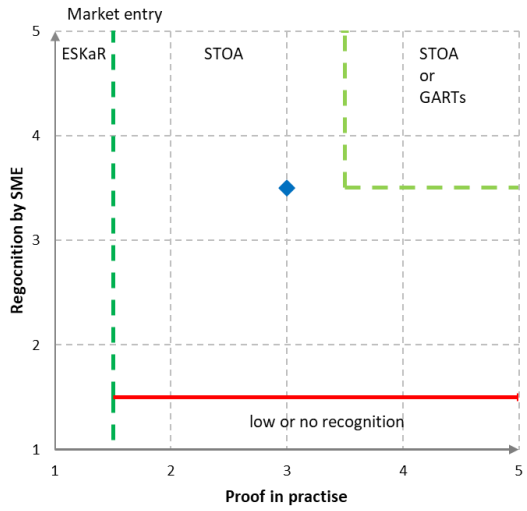
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.2.34 Encryption (Layer 1)

The lowest network layer of the OSI model is used for the physical transmission of messages over a medium between two points. Encryption is intended to ensure that the transmitted information cannot be intercepted by unauthorized persons. All connections and protocols of the network layers above are secured by common encryption at Layer 1. The protection provided by Layer 1 protection is particularly useful for transmitting easy-access media or large quantities of data. In the "VS Product Catalog of the BSI", a separate product class is designated for products with Layer 1 encryption.[20]

Against which threat(s) of IT security is the measure used?

Physical access to a transmission medium allows an attacker to listen in on the transmitted information. There is a high risk in particular with media that can be easily accessed, such as copper cables, power lines with Power-line communication (PLC) or radio. Optical fibers, which are used to transport large amounts of data over long distances, are also an attractive target for eavesdropping. Fiber optic cables are laid in routes, some of which allow very easy access.

The encryption of the payload data at the lowest network layer ensures the confidentiality of the information sent. In conjunction with hash functions or digital signatures, the integrity of the data can also be ensured.

Layer 1 encryption protects all data from the higher network layers, including metadata such as IP and MAC addresses. As a result, an attacker can't obtain information about communication relationships or behavior patterns of the users on the network. In the high-security sector, Layer 1 encryption is used to conceal traffic relationships.

What action (procedures, facilities or modes of operation) is described in this section?

Layer 1 encryption ensures the protection of all information transmitted between the endpoints of the physical connection. The two endpoints must authenticate themselves reliably and agree on a common, secret key or exchange a key between the end points in a protected manner. The key is then used with

[20] VS product catalog of the BSI, version 1.8 from 18.04.2024; German Federal Office for Information Security

a symmetric algorithm to encrypt or decrypt the user data. To significantly minimize the amount of data that could be decrypted in transit in the event that a secret key is compromised, renewing keys at regular intervals is recommended.

A connection at the lowest layer of the layer model can transport aggregated traffic from many connections at higher layers. The higher bitrate of aggregated traffic allows for faster clocking of encryption, resulting in low delays in encryption at Layer 1 compared to encryption of individual connections at higher network layers. The low latency of Layer 1 encryption is particularly important for time-critical applications, such as applications in the financial sector or for the transmission of highly accurate time information.

In practice, Layer 1 transmission systems are often used for longer periods of time than IT applications of the higher network layers, which are subject to significantly shorter innovation cycles. They must be designed for a long-service life and therefore also be prepared for the potential threat of future quantum computers. It is recommended to rely on quantum-safe methods of key exchange today. Various options are available for this, including post-quantum cryptography, QKD technology or hybrid methods that combine established methods and quantum-safe methods. When using the AES algorithm with a key length of at least 256 bits, the encryption of the payload is quantum safe.[21]

A key area of application for Layer 1 encryption is fiber optic networks that transmit large amounts of data over long distances. Due to the extensive infrastructure, access to the transmission medium cannot be reliably prevented. Access to the optical signals in the optical fiber is made possible by coupling elements, which are introduced as fiber or bending couplers during installation or operation. This allows the transmitted information to be read and interfering or falsified optical signals to be introduced.

For practical solutions for Layer 1 encryption of optical links, the OTN specifications form the basis. This allows standardized interface modules to be used. The use of optical amplifiers enables ranges of over 1,000 km. The key exchange is carried out via an auxiliary channel, which avoids a reduction in throughput in the useful channel. Aggregated traffic on Layer 1 is encrypted without any overhead, ensuring 100 percent throughput.

The high bandwidth of OTN signals allows for fast clocking of the encryptor, resulting in very low latency.

Encryption at network layer 1 allows the secure transmission of a wide range of protocols and interfaces in the payload. OTN technology provides the ability to securely transmit a variety of protocols and interfaces in the payload, including OTN, SDH, IP/Ethernet. It also makes it possible to transport special protocols between data centers or video studios.

The German Federal Office for Information Security (BSI) has approved transmission systems with Layer 1 encryption for the transport of classified information.

What protection goals are covered by the measure?

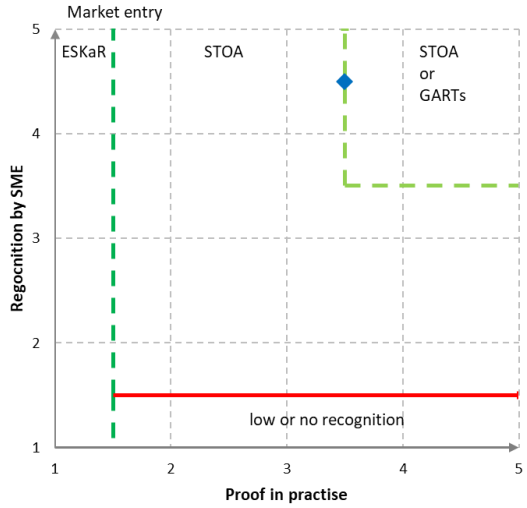
☒ Availability

☒ Integrity

☒ Confidentiality

[21] Making cryptography quantum-safe: Fundamentals, developments, recommendations; German Federal Office for Information Security (BSI), BSI-Bro21/01

Classification of the measure



3.3 Organizational measures

Since information and communication facilities are not always fundamentally designed for security and technical security is only effective if it is appropriately flanked by organizational and personnel measures, every organization needs a system of procedures, procedures and rules for managing operational information security, i.e. a so-called information security management system (ISMS).

An information security management system (ISMS) establishes and implements rules for the classification and handling of information worthy of protection. The ISMS is an important part of the company's general internal security management and runs through all important areas of the company. The ISMS includes procedures for regularly reviewing and documenting organizational and technical changes.

An important focus of the ISMS is the consideration of information security requirements in planned changes and maintenance of the important elements of the IT infrastructure. Another aspect is the regular training and sensitization of employees. In addition, the information security management system specifies how emergency preparedness is to be carried out and how to react to any security incidents. The aim of the ISMS is to permanently comply with and guarantee an efficient and always appropriate level of safety.

TeleTrusT has provided an actionable guide for information security management in its document "Information Security Management - Practical Guide for Managers". The document shows that information security management and the associated compliance and risk culture can be a strategic control instrument that illustrates the security situation at a glance.

3.3.1 Standards and norms

There are a number of international standards and norms related to information security. They can serve as a basis for aligning the company's security strategy and support the introduction of an ISMS. As with technical measures, the continuous change of organizational measures is a long-term task, so that referencing standards and norms is also possible in connection with the "state of the art". The ISO/IEC 27000 series is used as a reference point for other standards and norms. In some cases, there are overlaps, but these can usually be used as synergies, so that there is a positive influence in terms of information security.

The ISO/IEC 27000 standards world

The ISO/IEC 27000 series (sometimes referred to as ISO27k for short) is a set of information security standards. These standards are issued by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO/IEC 27001 is the best-known standard in the ISO/IEC 27000 series. It formulates the requirements to be met for an ISMS. In addition, there are other standards and guidelines for concrete implementation.

The ISO/IEC 27000 series contain the following essential contents, among others, each of which is managed as an independent standard and is summarized as a series of standards.

ISO/IEC standard	Content
ISO/IEC 27000	ISO/IEC 27000 series of standards overview document and terminology
ISO/IEC 27001	Requirements for an ISMS
ISO/IEC 27002	Guide to determining and implementing the requirements of ISO/IEC 27001
ISO/IEC 27003	Guide to the general requirements of an ISMS according to ISO/IEC 27001
ISO/IEC 27004	Guide to Monitoring and Measuring the Effectiveness of the ISMS
ISO/IEC 27005	Risk Management Guide
ISO/IEC TR 27019	Sector-specific guide as an extension of the measures of an ISMS for process control systems in the energy supply industry
ISO/IEC 27031	Information and Communication Technology Readiness Guide for Business Continuity
ISO/IEC 27034	Application Security Guide
ISO/IEC 27035	Information Security Incident Management Guide

Table 1: ISO/IEC 27000 Series Overview

Other standards and norms

Information security standards and criteria can be classified as enterprise, system, and product standards according to their level of consideration. According to their formulation, these can be divided into technical, less technical and non-technical standards.

Based on an earlier presentation of the D21 initiative, the above-mentioned levels of structure could be presented as follows:

	technical	less technical	nontechnical
Enterprise standard		BSI Standard 200/ BSI IT-Grundschutz	ISO/IEC 9000 ISO/IEC 20000 ISO/IEC 27000 ISO/IEC 22301 COBIT ISF SOGP
System Standard		ULD Privacy Seal, EuroPriSe-Privacy Seal,TÜViT TrustedProcess/Site/Product	
Product standard	ITSEC ISO/IEC 15408 (CC) ISO/IEC 19790 (FIPS 140) BSI C5		

Illustration 5: Levels of Structure of Information Security-Related Standards and Norms

As a standard for companies and public institutions (organizations), which is formulated in a non-technical language, there is a particular need to distinguish ISO/IEC 27001 from ISO/IEC 9001, ISO/IEC 20000-1, ISO/IEC 22301, CoBIT and ISF SOGP.

ISO/IEC 27000 ff.

The ISO/IEC 27000ff. series of standards includes several standards on ISMS. The core of the series of standards is ISO/IEC 27001, which describes requirements for an information security management system in the context of an organization (see 3.3.1.1).

ISO/IEC 27001 based on IT-Grundschutz

This involves the implementation of ISO/IEC 27001 with the help of the IT baseline protection methodology of the German Federal Office for Information Security (documented in BSI Standard 200-2) and the IT-Grundschutz Compendium.

The BSI Standard 200-1 defines general requirements for an ISMS. It is generally compatible with the ISO/IEC 27001 standard and also takes into account the recommendations of the other ISO/IEC standards of the ISO/IEC 27000 series of standards, such as ISO/IEC 27002. It offers interested parties an easy-to-understand and systematic introduction and guidance, regardless of the method they want to use to implement the requirements.

BSI Standard 200-2 provides the following with the procedure according to IT-Grundschutz:

- Concrete and methodological assistance for the step-by-step introduction of an information security management system
- Consideration of the individual phases of the information security process
- Solutions from practice, so-called "best practice" approaches
- Possibility of certification

The distinction between the "native" ISO/IEC 27001 implementation and the BSI's baseline protection approach can be found in the table below:

Category	ISO/IEC 27001	BSI IT-Grundschutz
Regulatory scope	Relevant standards< 100 pages	Baseline Protection Compendium> 4,000 pages
Requirements	Abstract and generic framework conditions	Concrete requirements for practical measures
Risk analysis	Complete analysis of each target object	Simplified analysis in the event of increased protection requirements
Measures	approx. 100 conceptual requirements	> 1,100 concrete actions
Certification	Certification	Auditor Attestations + Certification
Validity	3 years, annual surveillance audits	3 years, annual surveillance audits

Table 2: Differentiation ISO/IEC 27001 vs. BSI IT-Grundschutz

ISO/IEC 20000-1

This standard specifies requirements for internal or external organizations with regard to the provision of process-oriented services. Some of the requested processes (primarily Information Security Management, Incident & Event Management, and Service Continuity Management) overlap with ISO/IEC 27001. Traditionally, ISO/IEC 20000-1 is applied to IT service providers, while the scope of ISO/IEC 27001 can cover all types of organizations.

ISO/IEC 22301

The standard deals with ensuring business continuity management (BCM) and specifies requirements for business continuity management systems in organizations. BCM systems according to ISO/IEC 22301 also (but not only) have an IT reference. The topic of BCM is also dealt with in a topic area of ISO/IEC 27001, but only from the perspective of information security (i.e. the extent to which business continuity can be endangered by information security incidents).

BSI 200-4

The BSI Standard 200-4 provides a methodology for the introduction of a system for a BCM, which describes the step-by-step introduction of a BC management system with the establishment of an organizational structure with a maturity model. The stages: reactive BCMS, advanced BCMS and standard BCMS are defined, and a step-by-step approach is recommended.

ISO/IEC 9001

This standard specifies requirements for quality management systems, but also contains many information security aspects, for example with regard to the obligations to:

- Ensuring the availability of resources and information to carry out and monitor the processes
- Identification, retention, protection and retrieval of records
- Identification, provision and maintenance of infrastructure such as buildings, workplace and associated utilities, process equipment (including hardware and software) and supporting services (including communication and information systems)
- Protection of customer property, such as intellectual property, personal data, etc.

COBIT

COBIT is a method of controlling risks arising from the use of IT to support business-relevant processes. It is a "toolbox" for management oriented towards auditing and controlling, which defines result and performance measurements for all IT processes. COBIT describes several process areas, each with defined control goals, maturity model and measured variables. COBIT refers to all IT processes, while ISO/IEC 27001 focuses on the control of the information security process.

Standard of Good Practice (SOGP)

The Standard of the Information Security Forum (ISF) of Good Practice for Information is a "good practice" approach for corporate information security, which also allows "security benchmarking". The SOGP deals with several topics of information security (e.g. IT security management, business-critical applications, information processing, communication/networks, system development) from a business perspective and offers an alternative, partly complementary or complementary view to ISO/IEC 27001.

3.3.2 Security organization

The security organization focuses on protecting people, information, and assets from potential threats. A well-structured and functioning security organization is crucial to achieve a uniform level of security and to anchor security as an integral part of the company.

The tasks of the security organization include in particular:

- Identification and assessment of security risks (risk analysis)
- Development and implementation of risk mitigation measures (strategy)
- Continuous review and adaptation of security measures (monitoring)

The essential roles and responsibilities within a security organization are:

Role in the company[22]	Responsibilities
Managing Director (Managing Director), Board of Directors (CxO)	• Strategic responsibility (dedicated), but ultimately also overall responsibility for information security • Responsibility for all risk decisions
Chief Information Security Officer (CISO), Information/IT Security Officer (ISB/IT-SiBe)	• Tactical or (in part) operational control of information security • Support of the management in the performance of its IS tasks • Staff unit with direct reporting rights and obligations to the top management
Deputy / Area / Project Information Security Officer (ISO), Information (IT) Security Manager (ISM), Information (IT) Security Coordinator (ISK)	• Operational control of information security, if necessary tactical tasks for individual business units • Organizationally assigned directly to the CISO
IS management team, Security Steering Committee	• Permanent body to coordinate the planning and implementation of information security measures • Consisting of CISO, ISO(s), application representatives, business owners, data protection officers, top management representatives • Advisory and control function for the CISO
(Chief) Data Protection Officer ((C)DPO), Data Protection Officer (DSB), Data Protection Coordinator (DSK)	• Not necessarily to be seen as part of IS management, but ideally regularly involved in the IS management process as an important stakeholder in the topic of compliance
Audit Officer, Audit Manager	• Single point of contact for internal and external audits • Coordinates and controls the planning and execution of audits • Assisting the CISO on their behalf.

Table 3: Roles and responsibilities within a security organization

Regardless of the responsibilities listed in the table, overall responsibility remains with the management level (management, board). This is confirmed in the current legislation with a focus on information security and data protection in addition to the requirements already in force (e.g. AktG).

At least the ISO/IEC 27000 to ISO/IEC 27005 standards of the ISO/IEC 27000 series must be observed for the measures. If other applicable requirements, standards or results of risk analyses require it, further organizational measures may also be required.

What protection goals are covered by the measure?

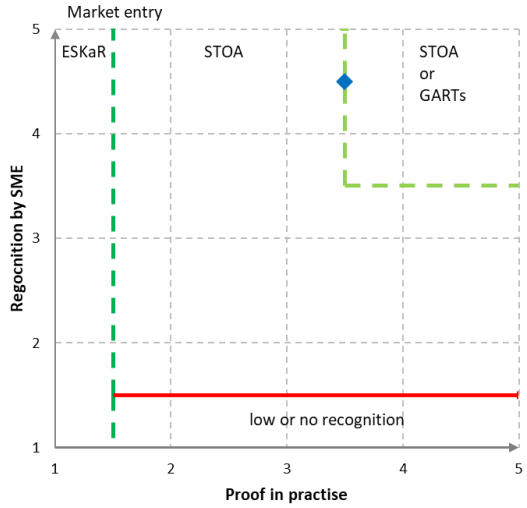
☒ Availability

☒ Integrity

☒ Confidentiality

[22] The role descriptions may vary in different companies

Classification of the measure



3.3.3 Information Security Management System (ISMS)

An information security management system (ISMS) is intended to ensure the confidentiality, integrity, availability and authenticity of information within its scope by establishing procedures and rules within a company and implementing security measures associated with them. This means that information security is permanently planned, managed and controlled in order to achieve, maintain and continuously improve the required level of security.

Requirements

The basis for the ISMS is the definition of the scope and the context in which the ISMS is to be established and operated. For the scope definition, internal and external requirements, expectations regarding the ISMS objective, involved parties as well as legal and regulatory requirements must be taken into account.

An ISMS requires a continual improvement process (CIP), which is implemented in the form of the PDCA cycle (Plan, Do, Check, Act) to ensure the maintenance of information security in the company. The following requirements must be implemented for the realization of an effective ISMS.

The support of the highest management level (management, board of directors, etc.) for the establishment and further development of an ISMS must be ensured, as decisions on the objectives, scope and implementation of the ISMS must be made from the highest management level and resources must be released. The support of the highest management level for the ISMS is provided by the adoption (signature) of the Information Security Guideline. This guideline defines the company's information security objectives within the scope of the ISMS, aligned with its business goals and strategies, and establishes the commitment of the highest level of management to continuously improve the ISMS. This is essential because overall responsibility for information security always remains with the highest level of management. The guidelines must be announced to all employees in the applicable scope of the ISMS for the organization.

In order to establish an ISMS and to implement technical and organizational security measures, a suitable, overarching organizational structure for information security must be in place in the area of application. The roles and responsibilities of all people and parties involved must be clearly defined. All people in the scope must be adequately considered in a training and awareness program according to their tasks, roles and responsibilities.

For the successful operation of the ISMS and to support the information security process, internal/external communication requirements and a process for documenting the ISMS (documented information and records) must also be defined.

One focus of the ISMS is risk management in order to identify and analyze (IT) risks for the organization and to make them as manageable as possible through appropriate measures or to reduce them to an acceptable level. To this end, risk management must be adapted to the company and integrated into the information security process.

Recommendations/Implementation

The following standards are recommended for the implementation of an information security management system (ISMS):

- ISO/IEC 27001:2022 The standard sets out requirements for a certifiable ISMS and describes the processes required for implementation, control, control and continuous improvement. If certification of the ISMS is sought, additional requirements from the controls listed in Annex A must be implemented.

- BSI Standard 200-1 The BSI Standard 200-1 describes the general requirements for an ISMS and combines the IT baseline protection methodology with the requirements of ISO/IEC 27001 in order to be compatible with it, which makes ISO/IEC 27001 certification on the basis of IT-Grundschutz possible.

- VdS Guidelines 10000 (VdS 10000) VdS Schadenverhütung GmbH, a subsidiary of the German Insurance Association, provides a practical, compact catalog of measures for the development of an ISMS especially for small and medium-sized enterprises. Certification by the VdS is also possible. The guidelines are based on the ISO/IEC 27001 standards and the BSI baseline protection.

- Information security management system in 12 steps (CISIS12)The "Network for Information Security in SMEs" – with members such as the Bavarian IT Security Cluster e.V. and the University of Regensburg – offers a scientifically supported model for the practical introduction of an ISMS in 12 steps for small and medium-sized institutions on the basis of the ISO/IEC 27001 standards and the BSI baseline protection. Certification is possible.

- The Austrian Information Security Manual describes and supports the procedure for establishing a comprehensive ISMS and, due to the chosen structure, offers an implementation aid for implementation in accordance with ISO/IEC 27001. The manual overlaps in significant parts with the BSI IT-Grundschutz.

Quality assurance

For the implementation of the PDCA cycle within the framework of the ISMS, audits must be carried out periodically (at least annually) to check whether technical and organizational measures are effective and are implemented and applied in accordance with the information security guideline. To this end, a regulation for reviewing and improving the information security process must be established, as well as a regular audit plan of at least three years to carry out internal and external audits. Audits must be carried out periodically in accordance with the audit plan and by professionally qualified people on an ad hoc basis. Reasons for audits are, for example, process changes, changes in scope, infrastructure changes or the identification of new, critical risks.

The highest management level must be regularly informed about the state of information security, e.g. derived from internal/external audits, and must evaluate the ISMS in the form of management reviews to ensure the suitability, appropriateness, effectiveness and continuous improvement of the ISMS.

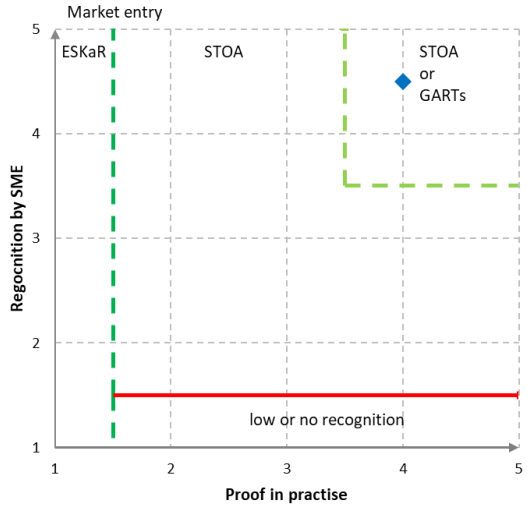
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.3.4 Secure software development

The security of an application must be considered throughout the software development process. Measures for secure application development must be taken into account regardless of the development method used. Process models and best practices for secure software development are described in BSIMM, OWASP SAMM, OWASP ASVS, the BSI guideline "Guide to the Development of Secure Web Applications" or ISO/IEC 27034, etc., and taught in the TeleTrusT Professional for Secure Software Engineering T.P.S.S.E. The essential protective measures within the software development process are listed in the individual chapters.

Requirements analysis

Secure application development starts with requirements analysis. The foundation of requirements analysis is a threat analysis. The (company) assets to be protected must be defined, and the threats to these assets must be described. The architecture of the application, especially its data storage and data flows, as well as its trust boundaries, must be taken into account. The risks of these identified threats must then be assessed, and countermeasures and security requirements for the application must be derived from this. A helpful method for identifying specific threats is a definition of so-called abuse cases. These describe specific attacks as well as the desired behavior of the application in the event of an attack. Further security requirements for the application arise, for example, from legal provisions or contractual obligations. These security requirements, like the functional requirements, are incorporated into the subsequent design phase of the software development process and also into the specification of the test cases for the later tests of the application.

The Volere template, which is often seen as the standard of the general requirements specification[23], already defines a number of security requirements that should be taken into account:

- 15a. Access Requirements
- 15b. Integrity Requirements
- 15c. Privacy Requirements
- 15d. Audit Requirements
- 15e. Immunity Requirements

Software Design

A secure design must take into account all security requirements in order to counteract the identified threats. The result of the design process is, among other things, the security architecture including a data handling strategy. A secure design takes into account aspects such as secure authentication, cryptographic requirements, error handling, system configuration, trust relationship between application

[23] https://www.volere.org/templates/volere-requirements-specification-template/

components, and the business logic of the application. Insufficient consideration of security in the design of an application is often the cause of weaknesses in the application, such as missing or incorrect authentication and authorization, and can only be eliminated afterwards with great effort. Other causes include keys or passwords built into the code, incorrect handling of sensitive data, or insecure error handling that provides useful information to the attacker. Adherence to so-called secure design principles helps an architect to achieve a robust design of his application. Examples of such proven design principles are Least Privilege, Defense in Depth or Secure by Default. Design principles such as Privacy by Default are becoming increasingly important, especially with regard to the EU General Data Protection Regulation. In addition, so-called design patterns and security best practices can be used by an architect, which, in contrast to design principles, offer a more concrete, yet language-independent approach to solving recurring problems. The design, or at least the design aspects relevant from a security point of view, must undergo a design review before the implementation of the application begins.

Implementation

Typical implementation errors, such as the unchecked processing of inputs including the output of this data, or the mixing of code and data, can lead to security vulnerabilities such as: injections, cross-site scripting or buffer overflows. Special programming guidelines help developers to pay attention to security during implementation. These should be individually tailored to the programming languages, libraries and frameworks used. When using frameworks, they must be used correctly so as to not undermine their security features. For example, it can be specified that only certain functions and objects may be used or that software modules may only be checked in after successful testing with a code analysis tool. Using static code checks, the source code must be automatically examined for typical implementation errors. The source code, or at least the parts of the source code that are relevant from a security point of view (according to the results of the threat analysis), should also be subjected to a manual code review.

However, weaknesses in the application can also result from the use of insecure components from other vendors. Therefore, such components must be carefully selected and the publication of security bulletins from these vendors as well as the CVE database of known vulnerabilities must be continuously reviewed. Such a check of third-party components should take place automatically with the help of a dependency checker tool. When using programs to deploy the application, such as container solutions, they must also be checked for known security vulnerabilities.

Software Security Testing

With the help of black box / grey box / white box tests as well as static and dynamic security scans, vulnerabilities in the application can be searched for. Where applicable, a combination of black box / grey box and white box testing, as well as static and dynamic security scans with specialized tools, is preferable to achieve the highest possible efficiency. For example, encryption algorithms used can be easily detected and evaluated by static analysis of the source code. In contrast, security gaps that arise through the integration of various components or only at runtime (such as during communication with an authentication service) can be easily detected by dynamic analysis of the system. Unlike manual security testing, security scans can be performed automatically as part of the software development process to ensure a security audit of each software version. In addition, the required security measures of the application must be checked during the testing phase, i.e., the extent to which the application is protected against the attacks identified in the threat analysis. The defined abuse cases are a good source for test cases.

However, these security tests do not provide an absolute statement about the security of the application. Security cannot be proven, as in functionality tests, by the fact that expected behavior corresponds to observed behavior. Safety is a negative criterion; it usually consists of preventing undesirable behavior. Here, the creativity of an attacker is almost endless. So, there may always be more threats, and thus, also other test cases that have not yet been considered. Therefore, penetration tests from the attacker's point of view and breach and attack simulations (BAS) run by appropriately trained personnel or with appropriately specialized applications are recommended.

Protection of source code and resources

To preserve the integrity of code and resources and thus protect the application from manipulation such as backdoors, Trojan horses or changes in the flow logic, source code control systems must be used and, if necessary, individual code parts must be assigned only to certain developers. Sensitive information must not be stored in source code control systems to prevent it from being unintentionally leaked

to the public. In addition, a secure development environment must be ensured by, among other things, restricting access rights and hardening systems, developers using only personalized user accounts, not working with admin rights, and being trained in security.

Software Certification

Before the software is delivered, it makes sense to check and certify it beforehand by a neutral body. While the functionality of the software has been ensured through testing, certification ensures that the architecture, requirements management, configuration management, and risk management are suitable for a secure development and, most importantly, a secure troubleshooting process.

In order to be able to eliminate vulnerabilities later, architecture and design should be designed in such a way that not only bugs can be fixed, but also faulty components can be replaced in an emergency.

For more complex software, requirements management is essential. The requirements should be checked (again) before delivery to ensure that they are clearly defined according to IREB (International Requirements Engineering Board). The implementation of requirements must be traceable back to the source code. In the simplest case, this can be done by assigning identifiers, which are then also used in code comments. This makes it possible to react quickly to vulnerabilities that become known.

Closely interlinked with requirements management is configuration management. Here, it must be checked whether a software version with source code and all its associated documents can be clearly assigned to a version (and later to a software release). When changing the requirements, one must be able to differentiate between documents that are up to date and adhere to the requirements and those that do not meet these criteria. Since documents are developed individually, each set of changes to a document are tracked by versioning. Therefore, in addition to the mere versioning of the documents, a so-called baseline must also be defined, which determines which documents belong together in which version number and thus correspond to a release. This makes it possible to see which software version, errors and vulnerabilities have already been fixed.

The first step inrisk management is to identify possible risks and hazards that could occur due to vulnerabilities. Risk management is particularly essential when human lives can be endangered. In the case of software certification, it must be checked before delivery whether there is a risk management system that completed the following tasks:

- Identified risks
- Categorized risks according to probability of occurrence and severity
- Defined measures to reduce risks
- Reclassifies the risks after the measures have been implementedat regular intervals and in the event of changes

If the software runs on a system network, the system network should also be certified.

Delivery of the software

A vulnerability in the delivery and setup of the software can nullify the result of all previous security measures in the software development process. Therefore, a secure delivery and setup process must ensure the integrity of the software that was released to prevent the production application environment from being compromised. The use of code signatures is a good way to do this, but attacks on the rolled-out deployed application can also be possible due to an insecure configuration of the application itself. Therefore, a secure configuration of the software in the production environment must be ensured, and unauthorized changes to the configuration must be prevented. As a security measure, suitable default settings (secure by default), the four-eyes principle and training for administrators are recommended. To minimize the potential damage of an attack, the application must have as few privileges as possible. Especially in container environments, applications are often run as root users unnecessarily, which should be avoided at all costs. It is also essential for the security of the application that it must always be kept up to date with regard to security updates.

Security Response

Since vulnerabilities can never be completely ruled out, every vendor must be prepared for security alerts and be able to react quickly. The vendor's security response process vendor describes their approach to dealing with security problems that have been identified. Security patches are time-critical and

must therefore be delivered promptly. This includes components developed in-house as well as known vulnerabilities in standard software such as libraries and frameworks. To motivate security researchers to report the vulnerabiresponsible vulnerability disclosure (RVD) or bug bounty programs are a good option. It is essential that reported vulnerabilities flow back into the software development process in such a way that they are fixed.

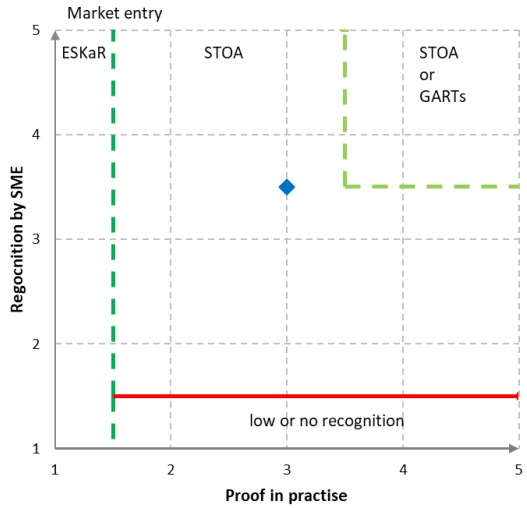
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.3.5 Process Certification

In order to successfully implement information security and data protection in a company, relevant processes must be identified and appropriate measures implemented. However, the implementation of such measures is only effective if their effectiveness is regularly reviewed. This verification can be done by internal or external resources. A special external impact, but not mandatory for all companies, is achieved through certification according to the current standards. This chapter describes the possibilities of process certification.

Context Information Security

In the context of information security, an ISMS can be certified according to ISO/IEC 27001 or (at least in Germany) on the basis of BSI IT-Grundschutz.

The ISMS certification audits have the following objectives:

- Checking the progress of an ISMS implementation
- Determining how well an organization's ISMS complies with standards
- Asesssing an ISMS's ability to meet legal, regulatory, and contractual requirements
- Testing the implementation and effectiveness of the ISMS
- Identifying weaknesses in the ISMS and potential improvements

Internal audits (so-called "first-party audits") within an area of application of the ISMS should generally be carried out at least once a year by the organization or on behalf of the organization. These audits are mandatory for ISMS certification. Each organizational unit (or any component of the scope such as

location, building, etc.) must be audited internally on a regular basis. In the case of an internal audit, it is essential that departments do not audit themselves, i.e., that audits are conducted by a separate organizational unit.

The so-called "second party audits" are external ISMS audits that are carried out by stakeholders who have a vested interest in the organization (e.g., their customers). If the external audits are carried out by independent auditing organizations, they are referred to as "third party audits". In the case of an outsourcing contract, appropriate supplier audits may be required.

However, the supplier (or outsourcing contractor) can also prove compliance with the information security requirements by means of a suitable certificate (e.g., ISO/IEC 27001 or ISO/IEC 27001 on the basis of BSI IT-Grundschutz).

If an ISMS is to be certified, the audit procedure must be carried out by an accredited certification body. Certification bodies for ISO/IEC 27001 have accreditation according to ISO/IEC 17021 and ISO/IEC 27006. An overview of accredited bodies for ISMS certification in Germany can be found on the website of the German Accreditation Body (DAkkS). The Federal Office for Information Security (BSI) is the responsible certification body for IT baseline protection.

In the certification audit, the audit team checks compliance with the requirements of ISO/IEC 27001 or BSI IT-Grundschutz. The audits must take into account the ISO/IEC 27002 and ISO/IEC 27005 standards (and any other industry-specific additions to the 27000 series of standards). Auditors from ISO/IEC 27001 certification bodies are required to consider the ISO/IEC 19011 and ISO/IEC 27007 standards as part of the audit process. In the case of audits in accordance with BSI IT-Grundschutz, the BSI's respective certification scheme must be observed.

Certifications according to ISO/IEC 27001 or ISO/IEC 27001 on the basis of BSI IT-Grundschutz have a validity period of 3 years and are checked at least annually as part of the so-called surveillance audits. If the certification is to be renewed for another three years, the organization must have successfully passed a recertification audit before the end of the three-year period.

Depending on the industry, sector-specific requirements may also have to be met. It must be checked whether the relevant sector-specific requirements require proof of a certified ISMS. In addition, further requirements can be defined that must be implemented and verified in accordance with the specification. An overview of the published sector-specific standards can be found on the BSI website.

In addition, there are other, partly industry-specific norms, standards and guidelines that also cover individual aspects of information security (e.g., VdS 10000, CISIS12, IDW EPS 980 nF, HIPAA, Euro Cloud StarAudit, CSA CCM, ITIL, SOC, PCI DSS, Fedramp).

Other advantages that speak in favor of ISMS certification are:

- Proof of appropriate risk assessment and treatment
- Independent third-party confirmation of the functionality of the ISMS
- Evidence of continuous improvement of the ISMS
- Reduction of liability in the event of incidents, because compliance with a harmonized standard in the EU gives rise to a presumption of conformity with the recognized rules of technology (standards) and the state-of-the-art
- External presentation in the context of corporate marketing for reputation vis-à-vis others

Context Data Protection

The implementation of a data protection management system (DSMS) is also a good way to check the effectiveness of measures in connection with the requirements of the European General Data Protection Regulation (GDPR). Although the GDPR does not expressly prescribe such a system, it nevertheless shows the need for such a system in many places. For example,[24] Art. 32 (1) (d) GDPR requires a "*procedure for the regular review, evaluation and evaluation of the effectiveness of the technical and organizational measures to ensure the security of processing*".

[24] Siehe ferner auch Art. 5 Abs. 2 DSGVO „*Der Verantwortliche (…) muss (…) Einhaltung nachweisen*“ und Art. 24 Abs. 1 DSGVO „*(…) sicherzustellen und den Nachweis dafür erbringen (…), dass die Verarbeitung gemäß dieser Verordnung erfolgt*“.

Since such a procedure requires a planned and structured procedure within the organization, i.e. requires the implementation of the classic PDCA model, the establishment of a DSMS is ideal for this purpose. If this is aligned with the elements of the ISO High-Level Structure, it can also be integrated into an existing ISMS based on ISO/IEC 27001.

Just like an ISMS, the DSMS can also be audited, and thus the maturity level of such a system can be determined. Based on the ISO/IEC 19011 guideline, audits can be carried out on the basis of an audit program and an audit plan. In principle, an audit can be carried out by the data protection officer. For larger organizations, the audits can also be carried out by expertly trained employees of the organization or consulting firms specializing in data protection.

As part of the so-called supplier audits, any of the organization's service providers can also be monitored.

Irrespective of the above, in the context of data protection, there is also the possibility of certification to obtain proof of compliance with the provisions of the GDPR (cf. Art. 42 para. 1 GDPR). However, under Art. 42 para. 5 GDPR, "data protection-specific certification procedures as well as data protection seals and test marks" in this regard must first be approved by accredited certification bodies per Art. 43 GDPR (in Germany, for example, the DAkks) or the competent supervisory authority. This has not yet been done.

However, as can be inferred from the wording of recital 100 of the GDPR, such "data protection-specific certification procedures as well as data protection seals and test marks" only refer to product, process and service certifications (see ISO/IEC 17065). In this context, the GDPR itself mentions, for example,

- proof of compliance with the obligations of a controller (cf. Art. 24 para. 3 GDPR);
- proof of compliance with the technical design and data protection-friendly default settings (cf. Art. 25 para. 3 GDPR);
- proof of sufficient guarantees from a processor (cf. Art. 28 paras. 5 and 6);
- proof of the security of the processing (cf. Art. 32 para. 3 GDPR);
- proof of suitable safeguards in connection with data processing in a third country (cf. Art. 46 para. 2 lit. f) GDPR).

A DSMS cannot be certified by means of "data protection-specific certification procedures as well as data protection seals and test marks" within the meaning of the GDPR. Nevertheless, these are complementary to a DSMS and can, in principle, be taken into account as proof of compliance with the GDPR when auditing a DSMS.

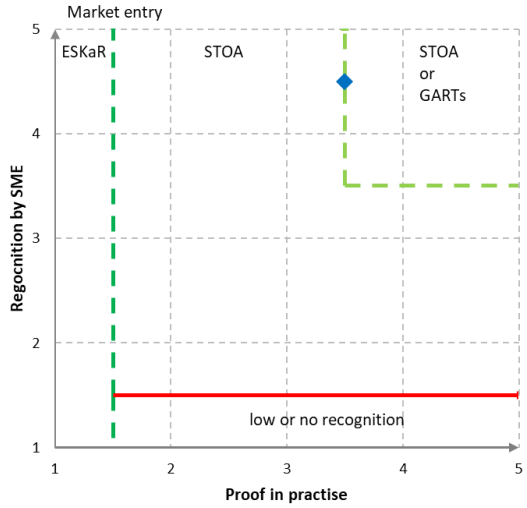
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.3.6 Vulnerability and patch management

The purpose of vulnerability and patch management is to identify and correct security and functionality weaknesses in software and firmware. Patches[25] are intended to fix identified vulnerabilities to prevent their exploitation. The vulnerability and patch management process includes assessing, identifying, evaluating vulnerabilities, and deploying them to all products and systems within an organization. For the vulnerability and patch management process, the responsibilities for implementation and for testing their effectiveness in the company must be defined.

- Assessment

In order to efficiently manage patches and vulnerabilities, the company's IT landscape must first be inventoried. Since this can change over time, such a survey must be carried out regularly and kept up to date. Components that are not located in the organization's internal network or cloud environment (e.g., smartphones and notebooks from service providers) must be managed via special guidelines. These guidelines are intended to encourage the owners of these components to ensure that the software version on their devices is updated independently or to connect them to the corporate network regularly.

- Identification and evaluation

In order to identify vulnerabilities, software fixes and threats, relevant sources of information (vendor websites, CERTs, CVSS databases, mailing lists of software and hardware vendors, third-party newsgroups, etc.) must be monitored, but professional enterprise vulnerability and patch management tools must also be considered. All those responsible for IT systems, applications, network components, etc., must periodically provide an overview/summary of the current patch status. From this, a report must be created for the assessment of the current vulnerabilities and patch situation and used to assess the current risk (e.g., CVSS score). The following solutions are available as treatment options.

- Handover to patch management to close identified vulnerabilities with a suitable patch (update)
- Defining workarounds (configuration adjustment, code analysis, etc.) to address the vulnerability
- Shutting down or isolating the affected system

If patches to fix the vulnerability are downloaded manually, their authenticity must be checked using standardized methods (cryptographic checksums, signatures or digital certificates), especially in case

[25] The three most important areas are
- Bugfix: Changes to the program source code to address a reported code defect.
- Hotfix: An unscheduled bug fix to address the urgent need for handing a code defect.
- Update: A regularly scheduled source code update containing functional enhancements and any bug fixes that coincide with the software release schedule.sometimes also the correction of errors

of downloads from the internet. Patches should be obtained directly from their respective vendors. Only in exceptional cases (e.g., in the case of integrated third-party products, such as runtime libraries) are patches from another verified trusted source permitted.

- Provision

After the authenticity of the patches has been ensured, they should be checked in test systems. If possible, the test systems should be equipped and configured in the same or comparable way as the production system.

Before the final implementation of the patches in the production environment, a backup of the affected systems should be created to enable the patches to be reinstalled in the event of an error. In the event of undesirable performance or limited functionality, troubleshooting measures should be identified and implemented.

To ensure that the implementation process runs properly, appropriate preparations should be made. This includes, for example, notifying all system owners and defining the time frame for distributing patches. The installation should also be announced to users so that they can complete their operational processes in time for the announced installation period.

Normally, the distribution of patches should be done automatically (e.g., with an enterprise patch management tool). Nevertheless, administrators might have to install individual patches locally. In this case, communication should be kept secure, and files should be exchanged using authentication checks.

As soon as patches are rolled out, progress must be monitored and communicated, e.g., in order to detect failed implementation attempts in time. For this purpose, suitable corrective measures must be carried out promptly.

- Handling exceptions

For systems or applications that

- can no longer receive updates from the manufacturer (so-called legacy systems),
- no operating system updates have yet been released by the manufacturer,
- for operational reasons (e.g., automation in process technology) no maintenance window can be made available on short notice,
- a recertification of the entire system becomes necessary in the event of an update,

technical measures must be identified and implemented. Since a shutdown or simple reconfiguration is usually not compatible with operational requirements,

- Network-side measures, such as separation, zoning, encapsulation or application firewalls as well as
- Network monitoring using an intrusion detection system

to protect against and detect exploitation of existing vulnerabilities should be implemented.

Manufacturer approvals

If the release of the manufacturer is required for the installation of patches (e.g., releases for patches of database or operating systems), available patches cannot normallyally be installed, since a loss of functionality would be possible and no warranty would be assumed by the manufacturer. For this reason, periods for the release and deployment of patches and updates or alternative workarounds for vulnerabilities must be contractually stipulated with the manufacturer.

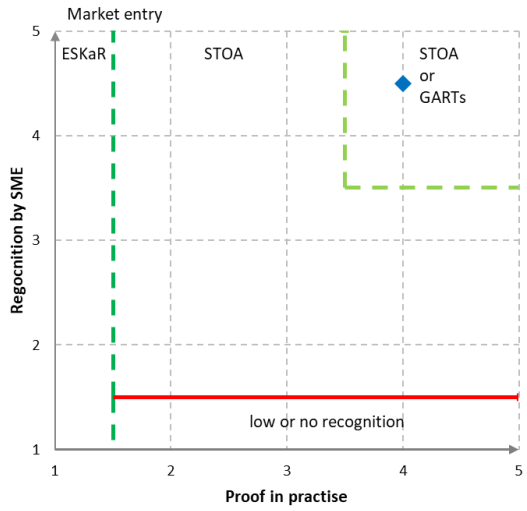
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the state of technology



3.3.7 Risk management

Risk management is an essential tool for managing corporate risks and thus the prerequisite for selecting appropriate risk-reducing security measures. In business practice, the use of security measures is decided by weighing up their costs and benefits. To determine the benefits, security risks must be identified and evaluated. Good and structured management of information security risks (ISRM) creates the necessary transparency that enables management to make appropriate decisions in this context. In addition, the management of information security risks is[26] a core element in the implementation and repeated updating of information security management systems (ISMS) or data protection management systems (DSMS).

Standards

The most important international standard for risk management in general is ISO/IEC 31000. The standard specifically applicable to information security risks is ISO/IEC 27005[27]. The latter is very closely based on ISO/IEC 31000 in terms of process but contains additional (non-normative) information on the identification and evaluation of assets, examples of threats and vulnerabilities, and methods of risk assessment in the context of information security. In Germany, BSI baseline protection is also relevant, in particular BSI 200-3 (BSI-GS for short). For industrial automation systems, the IEC 62443 Part 3-2 standard for "Safety Risk Assessment and System Design" is also available.

Depending on the regulatory environment, organizations may have to comply with other requirements, such as the European Network and Information Security Directive 2 (NIS-2) with the German NIS-2 Implementation and Cybersecurity Strengthening Act, the General Data Protection Regulation (GDPR) or the IT Security Catalog of the Federal Network Agency (IT-SiKat), which contain all supplementary requirements for risk management. Industry-specific security standards, the so-called B3S, have also been defined for individual industries with regard to the IT Security Act and provide recommendations for the implementation of risk management for critical infrastructure operators.

Process

[26] In this text, “IT risks” and “IT security” refer to risks and security for all types of information, not just electronically processed data.

[27] The ISO/IEC 27005 standard is currently being revised.

Risk management is a cyclical process (according to PDCA = Plan, Do, Check, Act). As conditions such as the threat situation, system vulnerabilities or the technological environment change, risk assessment must be kept up-to-date and its effectiveness monitored. Figure 1 shows the risk process according to ISO/IEC 31000.

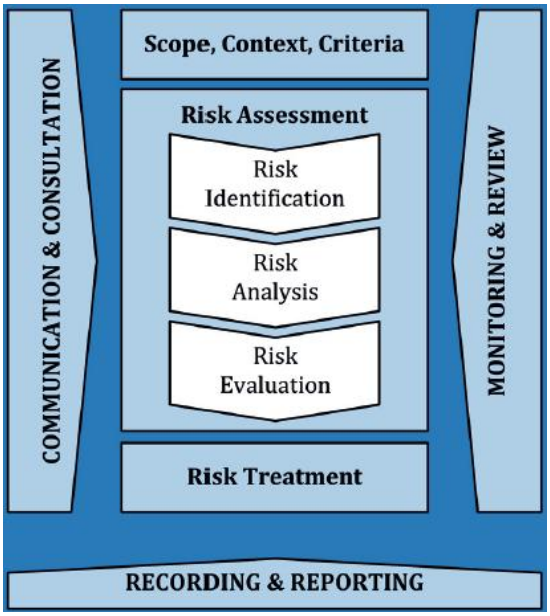


Illustration 6: Risk process according to ISO/IEC 31000

In the first step (**establishing context**), the basic prerequisites for ISRM are created. First, it is determined to which parts of the organization ISRM is applicable at all; if the ISRM is introduced within the framework of an ISMS, this usually results from the scope of the ISMS. The business processes that are to be included in the ISRM must be selected. Based on the business processes, the associated organizational units, IT and OT systems and applications, facilities for data and voice communication, service providers and also properties or buildings are taken into account. An ISRM organization is created with appropriate assignment of tasks (e.g. chaired by a risk manager), if this has not already been done within an ISMS or DSMS. It is also advisable to define interfaces between the ISRM and central corporate risk management, if available.

Hazards **are identified during risk identification**. Threats act against values (assets). In an ISRM, the values are primarily information, and secondary systems and components for processing and protecting them. During risk identification, the hazards to the assets are determined. According to the BSI's definition, threats are the interaction of threats (e.g. natural disasters, pandemics, burglary, hackers, insiders) and vulnerabilities (e.g. software errors, organizational deficiencies, technical defects). The challenge is to identify as many of these hazards as possible. Standardized risk catalogs such as those in Annex D of ISO/IEC 27005 or the risk overview from the BSI Baseline Protection Compendium provide support in this regard. However, these catalogs must be customized depending on the chosen context and the existing values. In this process, the cooperation of information security officers and experts – for example in a working group – is important.

Risk analysis means assessing the hazard in terms of its probability of occurrence and its potential for damage. As already mentioned above, it is rarely possible to fall back on solid figures for IT risks. Here, too, the assessments of experts, preferably from several disciplines, are decisive. Damage can be of different kinds (e.g. financial damage, endangerment of life and limb, impairments of supply or production / production, reputation, etc.). Since probability information is subject to a high degree of uncertainty and damage cannot always be clearly quantified, IT risks cannot usually be expressed as a concrete number (cardinal), but rather within an ordinal scale, for example "high", "medium", "low". Annex E in ISO/IEC 27005 provides helpful guidance on this type of classification. A hazard classified in this way is called a "risk".

Risks must be **evaluated** and appropriately **addressed**, for which there are several options. For example, you can wear them consciously (accept), insure yourself against them or introduce countermeasures (see chapter 6.4.4 in ISO/IEC 31000), but you should not ignore them. In this way, a conscious

decision is made. This decision must be made by a person who assumes appropriate responsibility, whether for the cost of action or damage if a risk materializes. This person is commonly referred to as a "risk owner."[28] If the risk is to be reduced, experts suggest countermeasures, the cost of which and the reduction of the risk form the basis for deciding whether to implement the measures. The "risk owner" then makes the decision on their implementation and the acceptance of the residual risk that remains after the measures have been implemented. Due to legal requirements for critical infrastructure operators or in the context of the GDPR, the "risk owner" is not completely free to accept or transfer risks without further treatment.

Communication, **reporting** (especially in the direction of management) and **monitoring** are supporting processes. They are already established within an ISMS or DSMS and must be applied to ISRM accordingly. In the presence of a central corporate risk management system, it is important that there is efficient communication and complementarity between it and the ISRM, and that criteria for escalating information security risks to the central corporate risk management system are defined that are understandable and acceptable to both sides.

Practical tips

The complete introduction of an ISRM is often a comprehensive task for companies (in terms of time and costs). Like other processes, ISRM is subject to a continuous improvement process, which at the same time means that you can't expect to establish a perfect process at the first attempt. Rather, an approach that is too heavyweight can prove to be a burden for the future: There is then a risk that the process will "fall asleep" in the long run or will only be implemented as a formally necessary relic without any recognizable benefit. In this respect, it is advisable to choose a pragmatic approach at the beginning, in which less attention is paid to completeness than to quality. It is important that the high-priority risks are identified, analyzed and adequately addressed, and that there is the widest possible consensus among the decision-making parties.

At the beginning, the identification of threats and their appropriate categorization are particularly challenging. You can stick to standard threat catalogs such as those in ISO/IEC 27005. Nevertheless, there is rarely a clear answer to the question, for example, of whether the threat of "lightning" should be classified under "force majeure" and treated as a major overall risk, as well as whether risks can be treated independently of each other, i.e. whether, for example, "lightning" should not be treated together with the risk of "power failure". Relationships can become arbitrarily complex, so that you have to accept certain inaccuracies. Inaccuracies come into play anyway via estimates of probabilities of occurrence. It is important not to lose sight of the goal, namely that the results of the risk analysis can be used to make a comprehensible decision as to whether there is a need for action or not.

Hardly less difficult is the assessment of probability of occurrence. It is advisable to use as many external and internal sources of information as possible. The former includes CVElists[29], manufacturer information, CERT services (e.g. from the BSI), the latter the evaluation of information security incidents, penetration tests, audits or awareness measures. The values should be adjusted regularly, e.g. at least once a year, to the current situation.

What protection goals are covered by the measure?

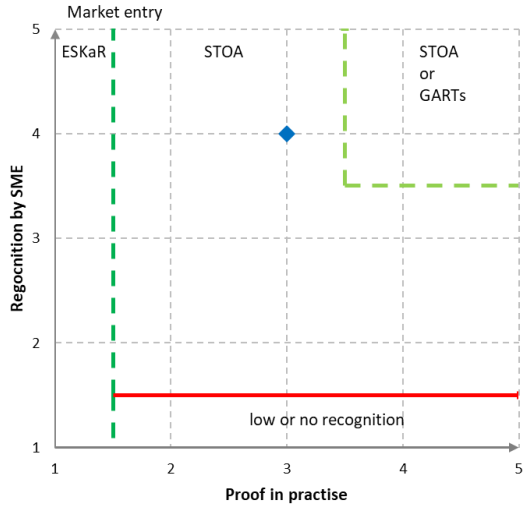
☒ Availability

☒ Integrity

☒ Confidentiality

[28] The term “risk owner” from ISO 27001 is also translated as “risk responsible person” or “risk holder”, depending on the responsibilities of the person in question.
[29] The Common Vulnerabilities and Exposures (CVE) is a standardized list of vulnerabilities and security risks of computer systems.

Classification of the state of technology



3.3.8 Personal Certification

The organizational measures include the deployment of qualified specialist personnel. This is especially true in business-critical areas and critical infrastructures (KRITIS). This is the only way to protect the company's assets and to meet the many legally enshrined requirements regarding the quality verification of the personnel employed.

Especially due to the increasing variety of technical solutions, it is imperative to continuously train all employees working in the IT sector on the basics and innovations. Employees should be trained and certified according to the respective activity and the needs to be derived from it, both with regard to the role to be fulfilled (e.g. administrator, developer, IT architect, auditor, information security officer, data protection officer) as well as with regard to the industry-specific (e.g. telecommunications, transport) and solution-specific (e.g. on-premises, cloud) characteristics.

The personal certification is used to prove professional qualification. This is because a personal certificate is usually only issued after specialist training and successfully passed the exam based on it.

Depending on the purpose and area of application, there are different certification programs on the market. Below are a few examples:

- **Administrators**
  - There are various manufacturer-dependent certification programs that are geared towards the use and configuration, as well as the administration of the respective product. These include, in particular, certificates from Microsoft, Oracle, Cisco, IBM, but also certification programs from cloud service providers such as Microsoft, AWS and Google.

  - ITIL practitioners and managers are manufacturer-independent and designed for the value-added processes of the information technology industry.

- **Software developer**
  - TeleTrusT Professional for Secure Software Engineering (T.P.S.S.E.) from TeleTrusT's key point of the T.P.S.S.E. certification is the expertise in how and where security aspects are integrated into software development. (https://www.teletrust.de/tpsse/)

  - ISC²'s Certified Secure Software Lifecycle Professional (CSSLP) is a vendor-neutral certification that demonstrates an individual's expertise in implementing security within a software development lifecycle. (https://www.isc2.org/Certifications/CSSLP)

- **Software Tester**
  - Certified Tester of various levels in various test areas of the International Software Testing Qualifications Board (ISTQB) (https://www.istqb.org/certifications/certification-list/)

- **IT Architects**
  - Certified Professional for Software Architecture (CPSA) by iSAQB The International Software Architecture Qualification Board (iSAQB) is an association of software architecture experts from industry, consulting and training companies, academia and other organizations. (https://www.isaqb.org/certifications/)

  - TOGAF, The Open Group Architecture Framework (TOGAF), provides an approach to designing, planning, implementing, and maintaining enterprise architectures. As an operational framework of the Government and Agency Frameworks group, the TOGAF offers the Architecture Development Method (ADM), a process model for the development of technical architecture.

- **IT Security Auditors**
  - ISACACISA's Certified Information Systems Auditor (CISA) is a globally recognized certification in the field of auditing, control, and security of information systems. (https://www.isaca.de/de/zert-start/international/cisa)

  - ISO/IEC 27001 lead auditor's focus is on the preparation and implementation of an audit of the Information Security Management System (ISMS). The certification is offered by various providers.

  - IT-Grundschutz Auditor Certification for conducting audits in accordance with BSI standards and the IT-Grundschutz Compendium.

- **IT Security Experts**
  - TeleTrusT Information Security Professional (T.I.S.P.) from TeleTrusTDhe content taught for the T.I.S.P. certificate covers the most important aspects of information security, technical and organizational measures, as well as German and European legislation. (https://www.teletrust.de/tisp/)

  - Certified Information Systems Security Professional (CISSP) from ISC²
    To obtain the certificate, expertise in security-relevant aspects from various areas of the so-called Common Body of Knowledge (CBK) must be proven. (https://www.isc2.org/Certifications/CISSP)

  - Comptia Security+ from the Computing Technology Industry Association (COMPTIA)The certificate focuses on basic knowledge of security concepts and technical and organizational measures. (https://www.comptia.org/de/zertifizierungen/security)

  - Certified Information Security Manager (CISM) from ISACA
    The focus is on the planning, implementation, control and monitoring of IT security concepts for specialists and managers (https://www.isaca.de/de/zert-start/international/cism1)

Especially for the German market, the Federal Office for Information Security (BSI) has also established a training series[30] for IT security experts with a focus on the BSI IT Baseline Protection Compendium. These are in particular:

  - BSI IT-Grundschutz Practitioner
  - BSI IT-Grundschutz Consultant
  - BSI IS penetration tester

[30] https://www.bsi.bund.de/

- **Data Protection Officer / Data Protection Coordinator / Data Protection Consultant**
  - To date, none of the consulting, shaping and controlling professions in the field of data protection has been certified according to a recognized independent certification procedure by an independent certifier in accordance with ISO/IEC 17024. Adequate data protection expertise depends on a variety of factors and cannot be taught by a single course. [31] For this purpose, more comprehensive training in the area of data protection is recommended. For instance:
    - Certified Information Privacy Professional (CIPP)This IAPP training focuses on data protection laws, policies, and standards in major international jurisdictions, the skills needed to manage data protection operations, and how to prepare for the certification exam. (https://iapp.org/train/)

- **Industry-specific certificates**
  - Telecommunication
    - Zero-Outage The contents of the Zero-Outage certifications include best practices and standards for delivering secure, reliable, and highly available end-to-end telecommunications IT services and solutions. (https://zero-outage.com/)

  - Transportation
    - Certificates for Operational ICT in Railway Operations
      The contents of the certifications for Operational ICT in Railway Operations include the best practices, standards and norms that must be taken into account in IT projects and IT applications in railway operations.
      (http://www.hmocs.de/)
    - RCS Academy (SBB)
      The content of the RCS Academy certifications covers the best practices, standards and norms that must be taken into account in IT projects and IT applications in the field of dispatching of railway operations, especially in Switzerland.

  - Automotive industry
    - TISAX auditor
      Trusted Information Security Assessment Exchange (TISAX) aims to protect information security in the automotive supply chain. It is strongly aligned with ISO/IEC 27001 but is specifically tailored to the requirements of the automotive industry.

In some cases, other European countries have their own individual certification programs that are not yet subject to uniform regulations. An overview of the certification programs of the European countries has been compiled by the European Cyber Security Organization (ECSO).[32]

What protection goals are covered by the measure?

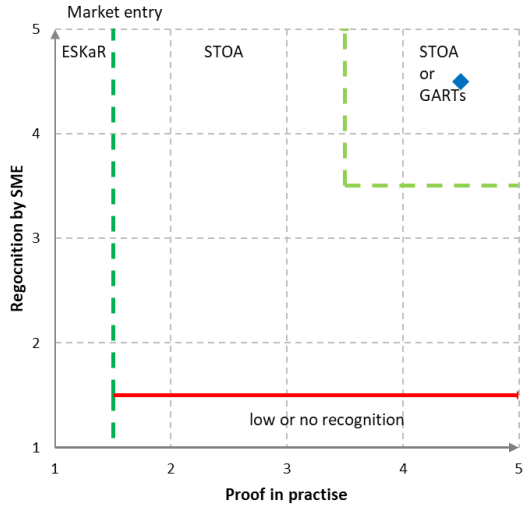
☒ Availability

☒ Integrity

☒ Confidentiality

[31] BvD, Berufliches Leitbild der Datenschutzbeauftragten, https://www.bvdnet.de/wp-content/uploads/2018/04/BvD-Berufsbild_Auflage-4_dt_en.pdf
[32] https://www.ecs-org.eu/documents/publications/5fad54a94cfac.pdf

Classification of the measure



3.3.9 Securing privileged user accounts

Privileged user accounts with extensive privileges are required to administer systems. Due to possible unauthorized or improper use, these accounts and associated rights pose a risk with great potential for damage. Therefore, appropriate regulations must be made to maintain proper IT system administration – in particular with regard to the assignment, use and withdrawal of administrative access rights.

In addition to interactive user accounts with administrative access rights, service accounts are usually used for applications or application services that do not require direct interaction on the part of the administrative user. This also includes the so-called service accounts (e.g. for cron jobs). The incorrect (usually too generous) assignment of rights to service accounts is a major vulnerability in most companies, which is also particularly targeted by attackers.

Administrative User Account and Access Rights Requirements

Guidelines and regulations must be defined for the use and handling of administrative authorizations and accounts. Before granting an administrative account to a user, the user should first accept and agree to abide by these policies and regulations. A violation of the defined guidelines and regulations must be clarified and have consequences.

A restrictive authorization strategy must be pursued, according to which access to resources is generally prohibited if this has not been explicitly permitted or released. For this purpose, a defined model or procedure for the assignment of authorizations should be applied. One possibility, for example, is the Role Based Access Control (RBAC) model. RBAC is a function-based access control, whereby authorizations are assigned on the basis of defined roles. Users are assigned to one or more roles and thus receive the access rights of these roles. At RBAC, the respective roles are defined on the basis of job profiles.

For the assignment of administrative authorizations, the need-to-know and least privilege principles must be observed. In the need-to-know principle, each person receives only the knowledge, authorization and/or possession of confidential information that is needed to perform his or her own tasks. With the principle of least privilege, each user receives exactly those rights that are absolutely necessary for the fulfilment of his or her tasks.

The assignment of administrative authorizations must be carried out in a defined and controlled process in which a request is approved and documented. Administrative rights may only be granted once this process has been completed.

Administrative access rights require you to create, and use dedicated administrative accounts that are different from user accounts for normal, non-administrative work. Activities that can be carried out without administrative rights may not be carried out by privileged accounts.

"Super administrators" with authorizations for all systems are to be avoided. In the case of existing standard accounts for administration, they must be deactivated, renamed and not used or used to a limited extent, depending on the possibility.

Each administrative user account must be uniquely assignable to a person. If this is not possible due to the system characteristics, the use of an anonymous administrative user account must be secured by accompanying organizational and/or technical measures and the handling of it must be recorded. Required group accounts for administrative activities must be precisely specified (in particular the permitted group of people) and the handling of them must also be documented and are only permitted in exceptional cases. The use of group accounts must be logged consistently.

Substitution rules must be defined for all administrative tasks. In addition, emergency accounts with administrative authorizations must be created, whose access data must be stored securely. The use of these accounts must only be possible to a limited extent and in a controlled manner (e.g. the four-eyes principle) and must be documented. For emergency accounts with multi-factor authentication (MFA), it is important to note that all factors for authentication must be present and operational or accessible even in emergencies.

If temporary administrative authorizations are granted, they must have a time/logical restriction and must be withdrawn when the necessity ceases to exist.

Administrative accounts with privileged privileges must be protected with a strong authentication procedure (coupling of several authentication characteristics, challenge-response or certificate-based procedures) in which the identity of the user can be clearly determined. User accounts with extensive privileges must be protected with authentication characteristics of various types (e.g. knowledge and ownership). If an authentication procedure appropriate to the risk is not possible, it must be checked whether additional technical or organizational measures are necessary for safeguarding due to the risk. The use of the same passwords for multiple administrative accounts is not permitted.

An up-to-date and complete documentation of all administrative accounts with their respective authorizations must be managed. This applies both to systems used, such as operating systems or device firmware, and to specialist applications, such as central applications.

For safety-critical activities, a division of activities or a separation of tasks must be implemented in accordance with the principle of separation of duties. This division or separation must be designed in such a way that the performance of safety-critical activities is tied to the presence of several users (e.g. by the four-eyes principle) or an activity is divided among several people who are not allowed to represent each other. In any case, administrative roles must be separated from controlling roles such as internal auditing.

All logins and activities carried out by administrative accounts must be logged so that it can be traced which activities were carried out by which accounts. To ensure the traceability of activities performed by administrative accounts, administrators must not be able to modify or delete log and audit logs of their own activities themselves. A review of these log and audit logs must take place regularly to check the administration’s activities for compliance.

Service Accounts in the Machine-2-Machine (M2M) Area

Administrators' accounts are often well secured, whereas the protection of service accounts is often neglected. By exploiting this circumstance, attackers very often succeed in the so-called "lateral movement", i.e. moving from one compromised system to the next (often more critical) systems.

Service accounts are often particularly vulnerable because:

- These accounts do not use multi-factor authentication (MFA)
- Saved passwords of these accounts can be read very easily (administrative rights required)
- The passwords of these accounts are often not changed and are not subject to new password policies, so they are often still very easy to compromise due to their age
- The passwords of these accounts are often known to many people and it is not documented which group of people has access to them
- These accounts often have much extensive permissions and therefore do not follow the least privilege principle

- These accounts are often used for too many purposes and thus add up an unnecessary number of permissions

All service accounts must be created and documented according to a defined procedure. Strong, randomly generated passwords must be used for these accounts, and these must only be made accessible to a small, defined area of people. If people leave the company with knowledge of the access data of these accounts or change functions, the passwords must be changed after an appropriate risk assessment.

For the protection of service accounts, interactive access should not be allowed for these accounts and any attempt to log in interactively with such an account should be investigated promptly. Separate, dedicated accounts should be created for each task and service (and not, for example, only one account per system) and the least privilege principle must be strictly adhered to. In order not to accidentally take over additional rights from other accounts, service accounts should not be copied from other accounts.

Recommendations/Implementation

For the management of administrative accounts and their access rights as well as for the implementation of regulations, the use of a Privileged Access Management (PAM) solution is recommended. Relevant standards are:

- ISO/IEC 27002:2022: The standard contains recommendations for the implementation of the measures required in ISO/IEC 27001 Annex A for the allocation, management and auditing/control of administrative accounts. If certification in accordance with ISO/IEC 27001 is sought, these measures must be implemented within the scope of the ISMS. Implementation instructions for these measures can be found primarily in sections 8.2 "Privileged access rights", "8.15 Logging" and "8.18 Use of utilities with privileged rights".
- BSI IT-Grundschutz Compendium (February 2022): In the OPS.1.1.2 module, the BSI IT-Grundschutz Compendium describes threats in connection with administrative accounts and derived from them, requirements for dealing with them.
- Austrian Information Security Manual: The Austrian Information Security Manual provides recommendations for the management of users, including administrative accounts. Recommendations can be found on the assignment, management and documentation of access rights as well as on the regulation of access options in cases of representation and emergencies.
- BDEW Whitepaper: Requirements for Secure Control and Telecommunication Systems 2.0: In addition to the requirement to comply with the need-to-know principle in the general requirements, the BDEW Whitepaper also contains the recommendation that applications and specialist applications must also implement user concepts in which administrator roles can be mapped and mapped with granular access control.

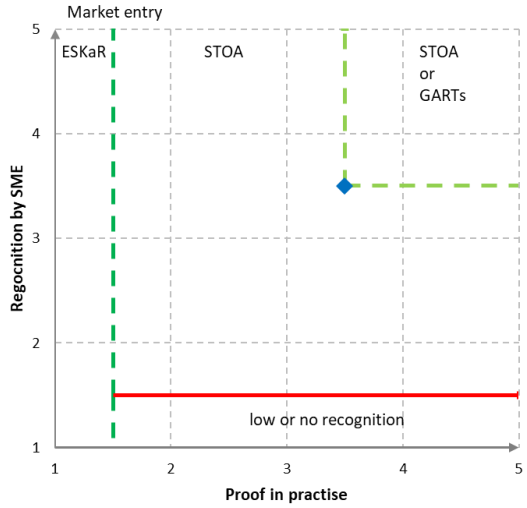
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.3.10 Dark Web Monitoring

Losing business-critical information can have serious consequences. Anyone who is informed about the loss can react. As in the real world, where stolen goods are traded on the black market, company information stolen on the Internet (e.g., information about vulnerabilities, findings from cookies used, stolen login credentials, financial transaction information) is traded on the so-called dark web[33] . This refers to a large number of separate networks (darknets) on the internet.

The dark web is used by attackers to exchange information with each other and to display and/or sell stolen company information. This usually takes place immediately after the attack. Technical compromises of companies, systems and networks often go unnoticed. They lead to a data leak or can be used to prepare for a targeted attack. Monitoring the dark web can therefore help to identify and document evidence of an attack on a company that has occurred or is imminent, and to initiate appropriate corrective actions based on the available information.

Against which threat(s) of IT security is the measure used?

Regular, targeted monitoring of the dark web[34] by commissioned specialized service providers or applications can help prevent planned or expected future attacks on a company (e.g., by a ransomware attack, illegal data theft or follow-up attacks by other attackers). This measure thus contributes to risk minimization. It can also uncover so-called supply chain attacks (also known as third-party attacks or value-chain attacks) in order to prevent an attack on one's environment from being carried out indirectly via third-party providers or suppliers or via the supply chain.

Dark web monitoring does not protect against the threat of compromise (intrusion by perpetrators) itself. However, the insights resulting from dark web monitoring can minimize risks to the affected organization by initiating appropriate response measures to prevent or at least limit further damage.

What action (procedures, facilities or modes of operation) is described in this section?

Manual analysis of publicly available information about a company and the current threat situation for the respective industry is carried out to subsequently set up automated rules and regulations that are individually adapted for the company.

These ensure regular monitoring (at least daily) of:

- Marketplaces and forums on the dark web (possible via special providers, among others)
- Published data leaks (e.g., Identity Leak Checker of the Hasso Plattner Institute[35])

[33] Also called Darknet or Deep Web
[34] As a special form of cyber threat intelligence (see chapter. 3.2.27)
[35] https://sec.hpi.de/ilc/search

- Public and non-public communication on the World Wide Web and on social media platforms, including relevant closed user groups
- Warnings from authorities from relevant bodies (e.g., BSI or US Cert)
- Media coverage

Manual analysis of the information and threat situation is iterated as needed to ensure continuous optimization of the regulations.

Due to the large amount of data expected, a high degree of automation and professionalization can usually only be achieved through a managed service. In addition, specialized data analysts with an investigative tactical skill set should be involved in these tasks.

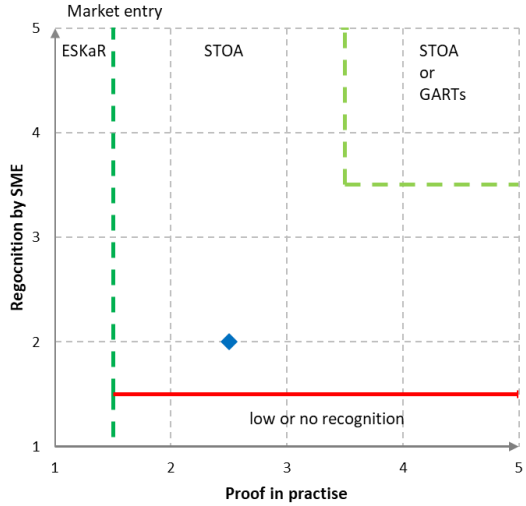
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.3.11 Working with service providers

Outsourcing services can be advantageous if service providers are more focused, more innovative and can provide better (or cheaper) service than the client or if the service provider is using specialized technology.

However, the commissioning of service providers is sometimes accompanied by considerable risks (e.g., dependency, loss of control and control options, risks for information security). In the worst case, these risks can endanger the client's existence. The more confidential or sensitive the data is, or the more the data is subject to restrictions (e.g., confidentiality, data protection), the greater the risk is to the client. Given these considerations, the selection, control, monitoring and verification of service providers are of central importance as an organizational measure.

The outsourcing of services (e.g., network administration) is accompanied by various threats to IT security (including information security), e.g.:

- Breach of security leading to the destruction, loss, alteration, or unauthorized disclosure or access to data
- Unlawful or inappropriate handling by third parties of the data provided for the purpose of fulfilling the contract

- Misuse of access rights obtained by the service provider and the resulting theft, loss or unauthorized disclosure of sensitive data
- Human and organizational error or misconduct due to non-compliance with agreed upon technical and organizational measures
- Legal risks (e.g., damages due to the service provider's actions and/or failure to act, fines or imprisonment, court orders)
- Financial risks (e.g., failure of the service provider due to insolvency)

To counter these threats, the following measures are recommended:

1. **Measures for the selection of service providers:**
    - Design or adaptation of the purchasing process with the aim of focusing on data protection and information security – e.g., by involving relevant bodies in the selection process at an early stage and setting minimum standards (baseline standards) based on individual or generally accepted standards (e.g., Trusted Computer System Evaluation Criteria (TCSEC))
    - Execution of requests for information (RFI) in a structured form with questions on information security and data protection, with the request for a binding statement from the service provider
    - Request for Proposal (RFP) from various service providers based on a detailed specification or scope statement, as well as individual data protection and information security requirements
    - Due diligence, i.e., careful examination with an assessment of all relevant legal risks associated with a legal transaction

2. **Measures for the management and review of service providers:**
    - In any case, it is advisable to define and delegate responsibilities internally with regard to the monitoring of service providers.
    - The type and scope of the measures depend on various factors, such as the size of the company, the complexity of the service level agreement (SLA) and the organizational structure, as well as the company's existing processes.
    - Establish and apply criteria for the continuous monitoring of the capability of service providers per established and contractually agreed requirements (in accordance with subsection 8.4 of ISO/IEC 9001).
    - Ideally, the measures are integrated into an IT risk management system that is embedded in the existing company processes (e.g., IT security management, compliance management, data protection management, etc.).

3. **Measures to monitor service providers:**
    - Prioritization of tasks and determination of inspection intervals
    - Determination of the type and scope of audit measures (e.g., on-site audit measures, use of questionnaires or commercial databases for service provider risk management, etc.by assessing the individual risk associated with the commissioning of the respective service provider based on the high probability of certain risks occurring, the degree to which the risk can be influenced and the effort required to do so
    - Service provider/supplier audits (IT security audits, data protection audits, physical security audits) during contract execution
    - Management of contracts, certificates and other documentation

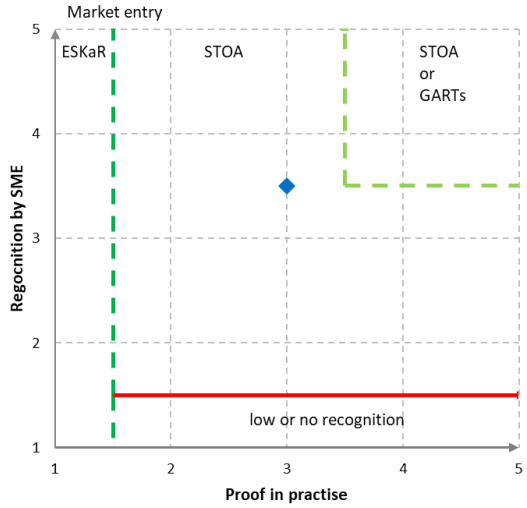
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.3.12 Software Bill of Materials (SBOM)

A software bill of materials (SBOM) is a list of components and their dependencies built into an IT application or service . This list is machine-readable and ensures transparency about the third-party components used. SBOMs can be used to determine vulnerabilities caused by underlying components.

Against which threat(s) of IT security is the measure used?

The measure is intended to enable the identification of the potential attack surface in so-called "supply chain attacks", which are carried out by exploiting security vulnerabilities in the components used (e.g., software libraries). Without an SBOM, there is no information about which components are used in an IT application or service, making identification of potential vulnerabilities difficult, if not impossiblet.

What action (procedures, facilities or modes of operation) is described in this section?

SBOM provides a complete bill of materials of all software components used in an IT application or service. This information allows to check against a list of vulnerabilities that may be present in a particular component and thus provide information about whether the IT application or service used may be affected by a particluar vulnerability.

Various data formats have been developed for SBOM. ISO standards exist for the SPDX1 and SWID2 formats, and the CycloneDX3 standard was adopted by OWASP. SWID and SPDX are primarily used for the unique identification of software for various purposes (not only security). CycloneDX, on the other hand, focuses on the security of applications and the analysis of supply chain components, even beyond software, including hardware components and cloud services. These formats are not compatible with each other.

SBOM is a central measure for defense against supply chain attacks. The U.S. administration mandated the provision and use of SBOM by suppliers to the U.S. administration through an executive order in May 2014, specified by the U.S. Department of Commerce (July 2021)[5] and NIST (February 2022).

The EU Commission has formulated the provision of an SBOM as one of the central security requirements as part of the Cyber Resilience Act.[36] In addition, BSI has defined the technical requirements for a software bill of materials (SBOM) with the TR03183.[37]

[36] EU CRA, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[37] BSI, SBOM-Anforderungen: TR-03183-2, https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR-03183-2-SBOM-Anforderungen.html

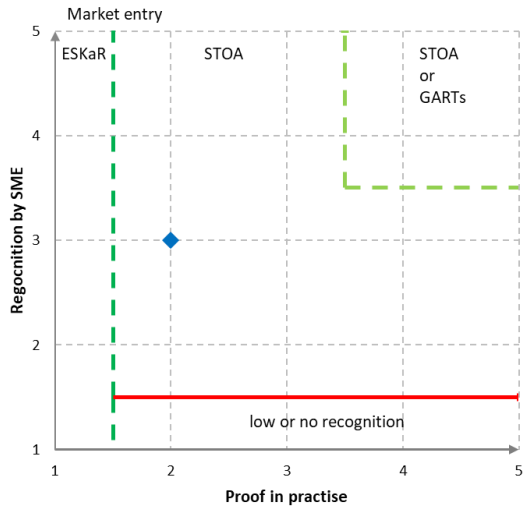
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.3.13 Geo-redundancies

The efficient use of the deployed systems and applications depends, among other things, on their uninterrupted availability. A failure of the IT infrastructure (e.g., networks, applications, storage, databases, computing capacities) has a direct negative impact on business operations. If high availability is required, the IT infrastructure must be configured for redundancy and made available on short notice in the event of an emergency. The redundancy must be designed in such a way that a failure of a single component does not lead to the failure of the entire IT infrastructure. Depending on a risk analysis, geo-redundancy can play a special role.

Against which threat(s) of IT security is the measure used?

The list of elementary threats[38] compiled by the German Federal Office for Information Security (BSI), also known as the G0 catalog, has become a standard that provides a structured overview of 47 potential threats and vulnerabilities in information systems. By standardizing the application of this catalog in protection needs assessment and risk analysis, organizations can develop a consistent understanding of risks and work more efficiently, including their assessment and prioritization. In addition, standardization promotes the comparability of security measures and improves communication between differentroles in the field of information security.

Excerpt of elementary hazards with a focus on threats to availability:

- Fire (G.01), Water (G.03), Natural Disasters (G.05)
- Power Failure (G.08)
- System, Network (G.09) and Services Failure (G.011)
- Physical damage, burglary (G.044), vandalism (G.044), theft (G.044), etc.

What action (procedures, facilities or modes of operation) is described in this section?

[38] BSI – Elementare Gefährdungen Stand 07.12.2020, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/Elementare-Gefaehrdungen/elementare-gefaehrdungen_node.html

To ensure high availability, the IT infrastructure used should be redundant. Here, "redundancy" means that a component is available multiple times (at least twice) in the same constellation and configuration. Which component of the IT infrastructure should be set up redundantly, or even geo-redundantly, is determined by the risk analysis.
An IT infrastructure deployment is considered to be redundant if its clone meets the following criteria:

- It provides equivalent resources.
- It is physically separate from .
- Its power supply, air conditioning and network connection are completely different.
- Its deployment has no effect on the original infrastructure.

In the event of a failure, e.g., due to storms, earthquakes, sabotage, power failures or component errors, the redundant IT infrastructure takes over part or all of the processing in order to maintain the operation of the entire system.

The failover configuration depends on the risk assessment and the potential amount of damage. The shorter the downtime that can be tolerated from an operational perspective, the more redundant components must be provided. This, in turn, leads to higher costs for their preparation and continuously updated provisioning.

Geo-redundancy also takes location into account as a geographical criterion. The choice of location must be considered individually, since it is based on the individual risk analysis of the company. An example of recommendations based on relevant criteria can be found at the BSI.[39] In particular, the spatial distances between redundant data centers can be seen there, which could be used as a rough guideline.

In the context of the increasing use of cloud services, it should be validated as part of a risk assessment whether redundancies of the operating components should be deployed.. Usually, these are not automatically created by the cloud service provider (CSP) but must be configured individually. Here, too, it makes sense to create a redundancy concept in advance that fits the risk assessment and readiness of the company.

Many cloud plans include customizable options for geo-redundancy that can be booked at rates based on the options selected. A trade-off between requirements and costs will most likely be necessary. Thus, the most important risk factors should be identified in advance before making a commitment.

Legal aspects must also be taken into account in the design and implementation of geo-redundancy. This is particularly relevant when using non-European service providers and data centers, since these may be subject to different jurisdictions and thus have the potential for different interpretations (e.g.,the CLOUD Act vs GDPR).

At the highest security level, an independent, further development of the CLOUD service should also be considered. This would require, among other things, escrow procedures, vendor-independent operation and the development of technical expertise.

What protection goals are covered by the measure?

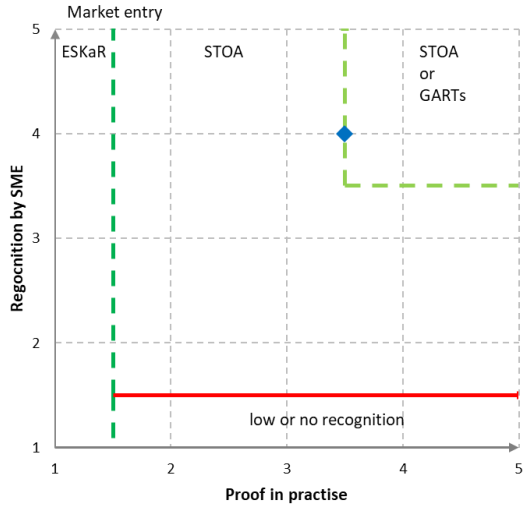
☒ Availability

☐ Integrity

☐ Confidentiality

[39] BSI - Standort-Kriterien für Rechenzentren (bund.de), https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Hochverfuegbarkeit/Standort-Kriterien_HV-RZ/Standort-Kriterien_HV-RZ_node.html

Classification of the measure



3.3.14 Raising user awareness

Employees are expected to comply with all information security-related rules and regulations in their daily work. Once workflows (such as opening an email attachment) have become a habit, it's hard to change. Therefore, new "safe" routines are needed. Such safe practices cannot simply be mandated. They need to be practiced. If employees are to implement measures consistently in the long term, they will need basic understanding and motivation

Against which threat(s) of IT security is the measure used?

- Promoting attacks (e.g., "social engineering", ransomware) due to insufficient awareness of information security and potentially harmful actions
- Compromise of accounts for attacks or exploitation by scammers
- Loss or disclosure of confidential data due to carelessness
- Failure to detect security incidents and insufficient action after a security incident

What action (procedures, facilities or modes of operation) is described in this section?

Organizations must ensure that employees[40] carry out their activities in compliance with information security rules. Awareness and knowledge alone are not enough for this. New *safe* behaviors are needed, that should be practiced until they have become part of one's daily routine. Also management should set a good example by adopting these routines.

The organization's approach to the topic of awareness must be structured. The following steps should be followed:

1. Selecting topics or a subject area
2. Defining the goals of the awareness campaign(s)
3. Implementing and verifying effectiveness

When **selecting topics or subject areas,** the results of one's own risk management and one's own information security goals should be considered first and foremost. Other aspects such as information security incidents in one's own or comparable organizations, a consideration of one's information values ("crown jewels"), one's corporate culture, requirements of important stakeholders, the analysis and evaluation of one's information security key figures and the results of audits should also be included in the selection.

[40] All persons who carry out activities under the supervision of the organization. When employees are referred to in this chapter, this is always meant in this broader sense.

The **goals of the awareness campaign(s)** should be formulated as concrete, operational goals. Measurability requires criteria that can be used to determine the extent to which the goal has been achieved (goal achievement criteria). The goals must be defined and documented before the start. In addition, a company-wide announcement of these goals should be considered if it could improve their achievement.

The **implementation** comprises nine steps, most of which build on each other:[41]

1. **Safety hygiene:** First of all, the own regulations must be checked for actual and practical feasibility. No one is expected to follow rules that cannot be implemented in the context of their work or can only be implemented with considerable difficulty. If this is the case, it should be checked whether the rules can be adjusted so that they can be implemented by all without undue complexity or hardship while still achieving the desired goals. Security can be improved most effectively when it is easy to implement and can be seamlessly integrated into existing processes.
2. **Information:** Employees need information about the existing regulations, i.e., they must be clearly conveyed and readily accessible.
3. **Sensitization:** Employees must be sensitized. The aim is not to focus on threat models and not to evoke fear, but to motivate them. This can be achieved by demonstrating professional and personal added value.
4. **Knowledge and understanding:** Employees must know and fundamentally understand how threats can exploit their "unsafe" behavior.
5. **Consent:** Employees should actively and, if possible, voluntarily agree to do their part, i.e., to change their own behavior.
6. **Expectation of self-efficacy:** Employees must be convinced that they can actually achieve the desired behavior and thus make an important contribution.
7. **Implement Skills:** The new skills will then be implemented. The new desired behavior is practiced. Employees are reminded that they have agreed to adopt the new behavior, what the old behavior looked like and why it is no longer practiced.
8. **Anchoring:** The new behavior must be firmly established and a relapse into old habits must be prevented. Anchoring can be implemented and supported by repetition, methods of voluntary forgetting or nudging[42].
9. **Safe behavior:** In the last step, the new safe behavior has become routine. To support this new behavior, a reward system can be introduced.

For each step, suitable tools and methods of support must be chosen. When selecting external service providers and services, care must be taken to ensure that the substeps of the implementation process described above are covered. If necessary, these must be supplemented by further measures.

All measures should be selected and implemented according to the needs of the various participants (software developers, IT, HR department, marketing, sales, etc.) in a way that is appropriate for each target group.

To ensure that the prerequisites for the implementation of the next step of process are met and to ensure that the defined goals are achieved overall, an effectiveness test should be carried out after each process step. If necessary, the step must be repeated or or more thoroughly implemented.

What protection goals are covered by the measure?

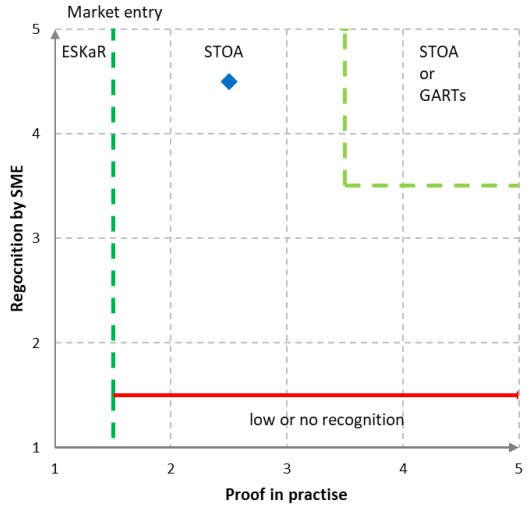
☒ Availability

☒ Integrity

☒ Confidentiality

[41] Human-Centred Security at the Horst Görtz Institute for IT Security, Ruhr Universität Bochum (https://hgi.rub.de/)
[42] Nudge or push, in the sense of thought-provoking impulse. Creating a situation that encourages people to adopt a desired behavior (including their own), e.g. positioning healthy food within sight and reach in a canteen.

Classification of the measure



3.3.15 Asset Management

An "asset" is any type of (asset information) value of an organization. Asset management is about the policies and processes that help to account for each asset throughout its lifecycle. From the point of view of IT (IT asset management), it is about the management of IT resources – hardware, software, but also data and cloud services used by the organization.

From the point of view of information security, the list of assets and owners provides the basis for protection needs analysis and helps to prioritize risk treatment and choice of protective measures. It is essential that the asset directory is not an exhaustive list but is to be understood analogously to the CMDB in ITIL and can be roughly divided into intangible and tangible assets.

From the point of view of IT security, IT asset management provides the basis for a comprehensive view of the IT landscape of the organization and thus for all IT security measures regarding IT assets; including risk assessment, patch management, security monitoring and zero trust.

Without structured asset management, organizations can be vulnerable to unauthorized access, loss, or destruction of critical information. After all, if the company's values are unknown, it is not possible to determine their need for protection and also not to initiate appropriate protective measures.

Asset management enables compliance with legal and regulatory requirements and promotes operational efficiency through a clear allocation of responsibilities and resources. In addition, complete asset management prevents the emergence of so-called "shadow IT", which can provide attackers with promising attack vectors that are not controlled by the company. Therefore, asset management should be integrated into the essential procurement processes.

The main tasks in asset management include:

- **Recording and inventory**: All company values should be systematically recorded, classified and inventoried.
- **Assign responsibilities**: A clear responsibility should be defined for each asset, including the responsibility to protect.
- **Classification**: Company assets should be classified according to their importance to ensure that they are appropriately protected.
- **Policies and procedures**: Implement clear policies and procedures for the handling and protection of media to prevent unauthorized distribution, alteration, or destruction.
- **Periodic Review**: Periodically review and update the asset management plan to ensure it meets current threats and business objectives.

The proven practices and recommendations are described in numerous standards and regulations, including:

- BSI Standard 200-2: Defines a structured approach to determining the assets and classifying the protection needs from normal to very high
- ISO/IEC 27001: This international standard for information security management systems (ISMS) emphasizes the importance of asset management.
- NIST SP 800-53: The National Institute of Standards and Technology (NIST) framework provides guidelines for managing information system resources.
- ISO/IEC 19770-1: Specifies the requirements for an IT asset management system in the context of the organization
- COBIT: ISACA's Control Objectives for Information and Related Technologies (COBIT) framework encompasses principles and practices for IT management, including asset management.

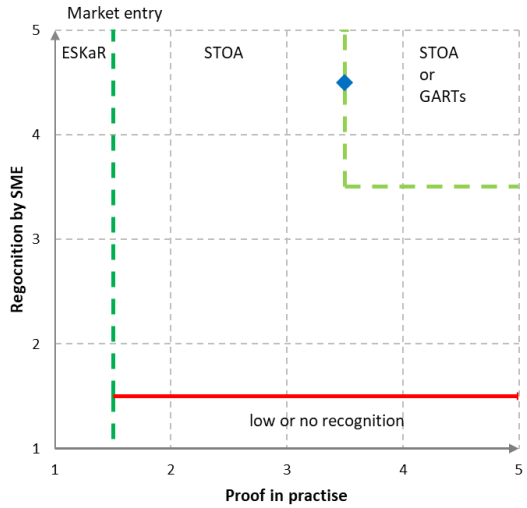
What protection goals are covered by the measure?

☒ Availability

☒ Integrity

☒ Confidentiality

Classification of the measure



3.3.16 Incident Management

Security incident management combines technical and organizational measures in response to detected or potential security incidents. In addition to recording, analyzing and managing problems, vulnerabilities or targeted attacks, it also describes and plans how to deal with such incidents, which also includes legal issues.

The aim of security incident management is to drive planning, identify and implement prerequisites in order to be able to take effective and efficient measures to protect the organization without delay in the event of an incident.

The main activities of incident management are:

- Capture: Identification and reporting of the incident
- Classification: Assessment and classification as a security incident
- Analysis: Investigation of the incident and determination of the extent
- Response: Implementation of mitigation and remediation measures
- Recovery: Return to normal operations and ensure integrity
- Follow-up: Documentation and analysis to prevent future incidents

Since incidents are often accompanied by a violation of the security protection objective of "availability", an initial qualified analysis and classification of an incident must be carried out initially. Based on this, the processing is then taken over by the respective specialist team, depending on the result. It makes sense to distinguish between functional and security incidents (or at least to label them separately), as both require different approaches, skills and measures. Functional incidents affect general operations and IT services, while security incidents specifically target the threat and breach of information security. The latter often require more urgent and specialized measures to minimize the damage and ensure the integrity of the systems.

For example, security incident handlers are required to have knowledge of IT security and the network architecture of the respective companies, as well as operational experience in the forensics of security incidents.

In order to ensure these requirements on an ongoing basis, the use of so-called SOC and CSIRT teams makes sense. The Security Operations Center (SOC) enables continuous monitoring of IT infrastructure, rapid identification of threats, and coordinated response actions. A Computer Security Incident Response Team (CSIRT) focuses on single, serious, and complex incidents. This significantly increases the efficiency and effectiveness of incident management.

Bringing together data sources in security information and event management (SIEM) systems or other security incident identification and assessment platforms is an important prerequisite for early threat detection and analysis. (Partially) automated processes, possibly using security orchestration, automation and response (SOAR) solutions, are recommended for fast response times.

In addition to defining and documenting a standardized security incident management procedure, employee training must also be ensured in order to strengthen the security awareness of staff and practice dealing with security incidents.

The establishment of a security incident team can be done using the ISO/IEC 27035, NIST SP 800-61 or CIS Controls frameworks.

The transition from a major service interruption can lead from incident to major incident and further to the convening of the emergency response team.

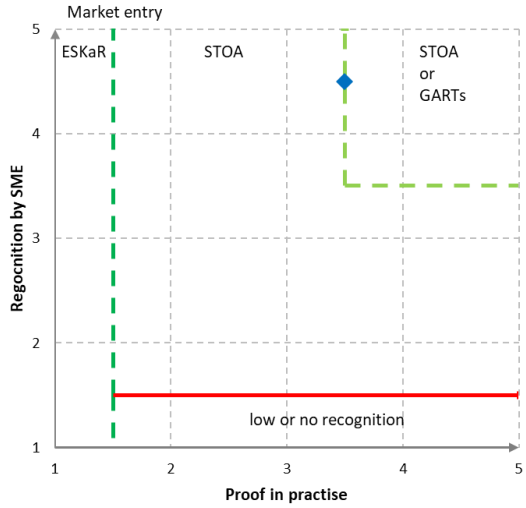
What protection goals are covered by the measure?

☒ Availability

☐ Integrity

☐ Confidentiality

Classification of the measure



3.3.17 Business Continuity Management (BCM)

Business continuity management (BCM) is a systematic approach that ensures that companies remain capable of acting even in crisis situations. It includes strategies and measures to secure time-critical business processes and minimize downtime.

The introduction of a BCM requires the support, alignment and provision of resources by the top management, this is documented by the BCM guideline and thus the BCM is put into effect.

BCM is essential to ensure an organization's resilience to various threats. Without a robust BCM system, companies can suffer significant financial losses, reputational damage, and operational failures in the event of disruptions or crises. The need for BCM stems from the wide range of potential threats that organizations face:

- **Natural disasters**: Events such as earthquakes, floods, or storms can severely damage a company's physical infrastructure and disrupt business operations.
- **Cyberattacks**: Attacks on IT infrastructure (e.g., malware, DDoS, ransomware) can lead to significant data loss and business disruption.
- **Technical failures**: Power outages, hardware defects or software errors can affect the operation of critical systems.
- **Pandemics and epidemics**: Health crises (e.g., COVID-19 pandemic) can severely limit the availability of personnel and resources.
- **Supply chain failures**: The increasing dependence on information technology (IT), functioning supply chains and external service providers (e.g. service, supply and supply companies) makes institutions vulnerable to disruptions. These disruptions impair the availability of business processes and thus pose a significant risk to the Business Continuity Management System (BCMS). A robust BCMS must therefore explicitly include measures to identify, assess and manage such supply chain disruptions.

BCM is used to look at the overall situation and resilience of the company. It mainly concerns the maintenance of time-critical business processes and the necessary technical and organizational components and measures.

An effective BCMS consists of several core components:

1. **Risk Assessment and Threat Analysis**: Identification and assessment of potential risks and threats to the organization. They form the basis for all further BCM activities.
2. **Business Impact Analysis (BIA):** Identifies critical business processes, looks at the impact of disruptions on business operations, and sets priorities for recovery.
3. **Strategy development**: It enables the development of strategies and measures to maintain or quickly restore business processes. In addition to the measures, it is essential that the roles

and responsibilities within the company are bindingly defined. It must be ensured that all parties involved know their tasks and can act effectively in the event of a crisis.

4. **Implementation and testing**: Finally, the developed strategies and contingency plans are implemented. Their effectiveness must be tested regularly and adjusted if necessary. Regularly reviewing and updating BCM plans based on the results of tests and real-world incidents.

The implementation of a BCM system can essentially be done along these frameworks:

- **ISO 22301**: This international standard represents the recognized standard for the establishment and operation of a business continuity management system (BCMS). It structures the requirements for the planning, implementation and monitoring of a BCMS according to the ISO requirements for management system standards and forms the basis for the possibility of certification of a BCM system.
- **BSI Standard 200-4**: The BSI Standard 200-4 offers comprehensive, practical guidance on how to set up a BCM organization and implement a BCMS, especially in connection with IT baseline protection based on ISO 27001. Standard 200-4 is provided free of charge by the Federal Office for Information Security with extensive tools.

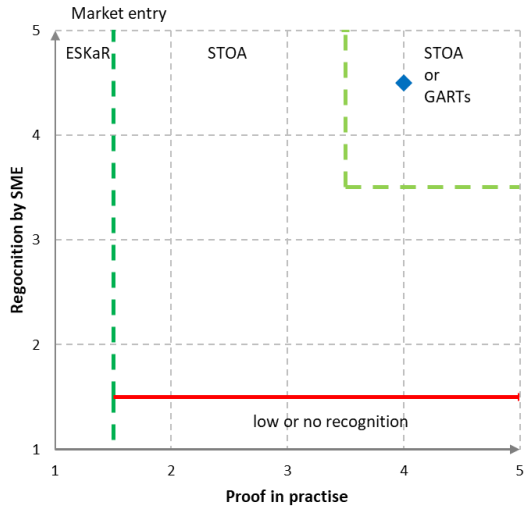
What protection goals are covered by the measure?

☒ Availability

☐ Integrity

☐ Confidentiality

Classification of the measure



3.3.18 Emergency and crisis management

Emergency management refers to the planning and implementation of measures to respond quickly and effectively to IT emergencies, such as system failures or cyberattacks. The goal is to minimize the impact of such incidents and restore business operations as quickly as possible.

Crisis management, on the other hand, involves responding to more serious and often unpredictable events that require a flexible and comprehensive approach. It is about making strategic decisions to ensure long-term stability and security of the organization.

An emergency can lead to a crisis or be declared as such. This requires a standardized procedure and coordinated criteria according to which the corresponding criticality level and the process protocol provided for this purpose are activated.

A (cyclical) crisis management process consists of:

1. Situational awareness/control
2. Location assessment
3. Planning and selection of measures
4. Delegation and implementation of measures

Although business continuity management (BCM) and emergency and crisis management are very similar, they differ in their approach:

	BCM	Emergency crisis management
Focus	Long-term business continuity assurance	Short-term response and management of acute threats
Goal	Meeting the availability requirements of critical business processes	Protecting people and assets, minimizing damage
Activities	Preparation and testing of business continuity plans (GFP) for critical business processes and services	Immediate response, operational and strategic decisions during a crisis
Scenarios	Contingency plans are in place for failure scenarios and processes are known.	Unknown or particularly serious scenarios for which no contingency plans are in place.

Table 4: Differentiation between BCM vs. emergency and crisis management

A structure for the first hours and days of a crisis should be agreed and documented. In particular, the alerting and escalation, the composition and ability to work of the crisis team as well as measures for the rapid restoration of business processes should be recorded.

With the help of the parameters collected in a BIA, the damage potential of a failure can be assessed. Standardized assessments together with the consideration of the time horizons help to define the so-called unsustainability level and to derive appropriate measures from it.

Note: Important parameters and terms of BCM and emergency management are defined in the glossary of BSI Standard 200-4: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_BCM_Glossar.pdf?__blob=publicationFile&v=3

Crisis definition and activation of crisis organization

It must be clearly regulated who is allowed to declare the current situation a crisis, taking into account all the information available at the time, and thus activating the defined processes and resources. This decision can be made according to previously defined criteria regarding the impact and scope of the incident. Essentially, whenever the treatment of the incident exceeds the possibilities of the established structures, and the effects cannot be foreseen either in terms of time or effects. When the crisis is declared, the crisis team headed by the crisis manager, takes responsibility for managing the situation.

Crisis team and responsibilities

The composition of the crisis team may vary depending on the nature of the crisis. In addition to the crisis manager, it is advisable to provide at least one member of the management in order to make the crisis team largely capable of making decisions without the need to consult other committees. It makes sense to form a core crisis team with the necessary roles in every crisis. This core team is supplemented by other roles depending on the situation. Depending on your needs, the following can be considered:

Core	Situational complement
• Management • Communication • Right • Protocol (situation report)	• Representatives of critical departments • IT • Communication • Staff • Finances • Right

	• Privacy • External Crisis Consultants • Works council • Secretary

Table 5: Composition of the crisis team

For each position in the crisis team, clear deputy regulation and accessibility must be defined in order to ensure the ability to act even in the absence of individual members.

Situational extensions are possible at any time with the aim of involving all the necessary competencies that are necessary for a quick decision on how to proceed.

Communication and information sharing

In the event of a crisis, all internal and external stakeholders relevant beyond the crisis team must be informed via previously defined communication channels, involved in the work of the crisis organization and informed of the current situation. A crisis communication plan should include the following aspects:

- Internal communication: regular updates to employees
- External communication: media management, customer information, communication with authorities
- Pre-built communication templates for various crisis scenarios
- Determination of speaker roles and communication channels

Reporting Requirements and Legal Requirements

Various reporting obligations must be observed that must be observed:

- Operators of critical infrastructures (KRITIS, NIS2) must report incidents to the Federal Office for Information Security (BSI) in accordance with the specifications and reporting channels
- Depending on the industry, reporting obligations may also be relevant. For example, for telecommunications companies (Federal Network Agency) or financial institutions (BaFin)
- If access to personal data cannot be excluded, a report must be made to the competent data protection authority within 72 hours in accordance with the GDPR

In addition to these legal or regulatory reporting obligations, internal reporting obligations should also be prepared and taken into account accordingly (cyber insurance, reporting to the police, ...). It is important to check these reporting obligations regularly, at least annually, to ensure that they are up to date and, if necessary, to adjust them. For each reporting obligation, specific contact persons or bodies should be named, and their contact details should always be kept up to date.

Regular review and adjustment

Crisis management plans should be available, regularly reviewed and updated, to respond to new challenges or changes in the corporate structure or legal environment. This review can be carried out in regular (at least annual) exercises (e.g. Desk exercises, plan meetings, staff exercises,...) to ensure the effectiveness of the crisis processes. Likewise, after the end of a crisis, follow-up should be carried out in order to update the existing plans on the basis of the knowledge gained on effectiveness and potential for improvement.

The BSI emergency card[43] and the emergency manual have proven to be very helpful [44] . They offer operational templates with the most important data at a glance in order to be prepared for the worst-case scenario.

[43] BSI Notfallkarte: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Unternehmen-allgemein/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html

[44] BSI Notfallhandbuch: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Standard200_4_BCM/Standard_200-4_Vorlage_Notfallhandbuch.html

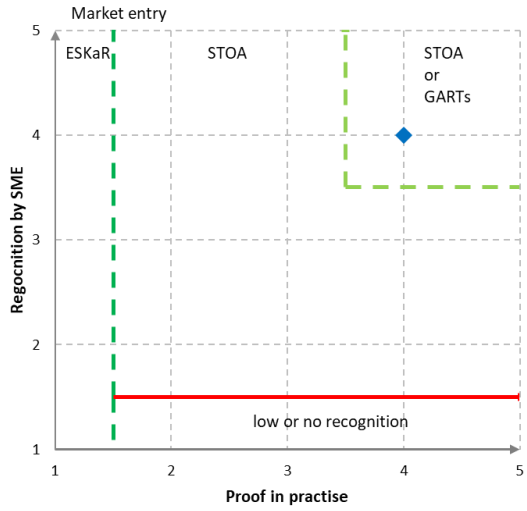
What protection goals are covered by the measure?

☒ Availability

☐ Integrity

☐ Confidentiality

Classification of the measure



3.3.19 Emergency drills

The number of cybersecurity attacks and threats continues to increase worldwide. Accordingly, the question of "whether a company is attacked" is obsolete. Rather, companies must prepare for an attack and the organizational measures resulting from it and test and practice them regularly.

As part of an emergency drill, potential effects of a successful cybersecurity attack can be simulated. Various forms of emergency exercises, such as tabletop exercises, crisis team exercises and full exercises are possible. Emergency drills can be planned in isolation, e.g. within the department, or integrated (emergency joint exercise). Exercise as a simulation game allows you to test how to deal with a fictitious attack and to test your own reaction skills. The aim of the exercise is to identify possible organizational weaknesses in order to avoid them in an emergency.

The emergency exercise will test the handling of the previously defined security threats and, in particular, the effectiveness of existing organizational measures and identify weak points. The participants are confronted with an unknown situation that they have to deal with discursively (e.g. through questions or tasks and actions). In particular, such an emergency drill enables:

- deal with concrete threat scenarios in a targeted exercise before an emergency
- Have discussions about and test existing policies, contingency plans and procedures
- Develop organizational measures and test the extent to which these measures work against certain threats
- Testing of existing organizational measures
- Create awareness of roles, competencies and responsibilities
- Examine responsibilities and lines of communication and put them to the test
- To promote willingness and to rehearse familiarity with procedures.

The implementation of safety drills requires an individual incident scenario designed for the respective organization and aimed at its specificities. Depending on the needs, the individual circumstances of the incidents to be carried out can be increased in their complexity and extent during the exercise.

Goals should be set in advance of the safety exercise to validate the effectiveness of the exercise. For example, the following goals can be defined:

- Processes of information exchange between stakeholders are to be practiced
- The effectiveness of the emergency plan is to be tested
- Measures against a specific threat are to be developed
- Crisis communication, internal and/or external, is to be tested.

To identify the most relevant threat for the scenario, risk analysis and threat modeling can be used. If feasible and sensible, technical tools can also be used to measure the scenario to be tested and evaluate its effectiveness.

The emergency exercise should take place in a familiar, informal and error-tolerant setting, with sufficient process orientation. Since the emergency drill focuses on testing organizational measures in the context of a successful attack, there is no need for a virtual or secured digital network with real tools and techniques.

However, organizational knowledge, expertise in the field of information security, communication skills and an objective ability to evaluate as well as the necessary creativity are required to develop scenarios that are realistic and fit the goal of the exercise at the same time.

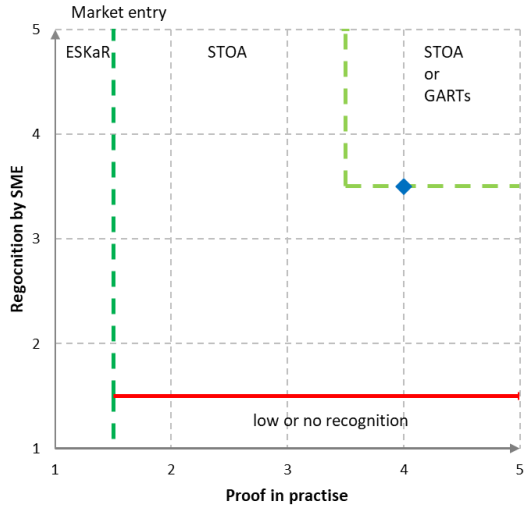
What protection goals are covered by the measure?

☒ Availability

☐ Integrity

☐ Confidentiality

Classification of the measure



3.3.20 Technical security review

In various places in the guidance document, there is talk of audits, e.g. in the audit of information security management systems such as ISO 27001 or BSI baseline protection. The vast majority of audit forms are process audits and are provided on the basis of evidence in the form of documentation. However, it is a good idea to supplement audits with technical security checks. While audits demonstrate correct and meaningful processes, technical safety reviews derived from them provide evidence of their actual effectiveness. After all, even with a perfectly documented firewall and an established change process, serious security gaps can be hidden.

The technical safety checks presented here are one-off tests carried out in the context of audits. Ongoing technical measures that can be established as a continuous process in the company – such as permanent vulnerability scans – are not the subject of this article.

Depending on the environment, there are a variety of possible test methods. The following options are therefore not exhaustive and should be selected by auditors with appropriate technical domain knowledge. The implementation should always be carried out by experienced experts whose daily work includes technical safety checks.

Configuration analyses

Configuration analyses ideally compare existing security concepts with established configuration and change management. As a rule, these are random inspections. As a result, differences between specifications and technical implementation are to be revealed. The following exemplary questions can serve as a guide:

Range	Question
Active Directory	Are the password policies configured correctly?
Backup Configuration	Are backup jobs set up according to the documentation and are they adjusted according to change management?
Client Management	Are all clients in patch management managed and up-to-date?
Cloud Configurations	Are IAM roles and permissions in cloud services (e.g., AWS IAM or Microsoft Azure RBAC) implemented in accordance with security concepts?
Database Management	Are user accounts in productive databases correctly documented and role-based with minimum necessary rights?
Printers & All-In-One Printers	Are access restrictions enabled, and is network access limited to what is necessary?
Email Gateways	Are filtering and protection mechanisms (e.g., SPF, DKIM, DMARC) active and correctly configured?
Firewall Users	Are all users documented? The verification of the individual user accounts and the secure retention of the "Admin" password is carried out separately in the process review.
Firewall Rules	Are these clearly assignable to the documentation and the change requests?
Mobile Device Management	Are mobile devices (e.g. smartphones and tablets) registered, managed and encrypted?
Monitoring systems	Are backup jobs set up according to the documentation and are they adjusted according to change management?
Monitoring systems	Are all critical systems correctly integrated into the monitoring and are alarms triggered according to defined thresholds?
Configuration	Do services, protocols and ports comply with the approved and documented specifications?
VPN access	Is the second authentication factor activated everywhere possible?
Web server	SSL/TLS configurations meet documented minimum requirements. Have you disabled deprecated protocols (for example, no deprecated protocols such as TLS 1.0)?
Wi-Fi configuration	Are corporate Wi-Fi networks protected by WPA2-Enterprise or higher? Are guest networks sufficiently segmented?

Table 6: Exemplary questions in configuration analyses

Curing Checks[45]

As part of hardening reviews, the implementation of minimum technical standards on systems and applications is evaluated. The aim is to check whether established hardening specifications (e.g. CIS

[45] See also chapter “System hardening”

benchmarks or own internal standards) have been consistently implemented. Differences between the configuration specifications and common practices are identified. Exemplary questions are:

Range	Question
Application Curing	Have default passwords been removed and secure configuration options chosen?
Backup systems	Are backup servers and storage especially hardened, such as restrictive network access and separate authentication?
Client Hardening	Is access to administrative functions restricted for users? Are the permitted applications (whitelisting) available and correctly configured?
Container hardening	Are container images sourced from trusted sources and updated regularly? Are unnecessary services within the containers disabled?
Mobile Devices	Is local storage encryption active? Are device management policies (e.g., remote wipe) in place?
System hardening	Are unnecessary services deactivated because they are not used, and secure configurations set?
Virtualization platforms	Is access to hypervisor management systems (e.g., vCenter) protected and restricted to authorized individuals?

Table 7: Exemplary questions in hardening tests

Automated vulnerability scans

Automated vulnerability scans systematically record known vulnerabilities in the technical infrastructure. They should be used in a targeted manner to get an overview of the current vulnerability status. Examples:

- **Backup infrastructures:** Check for vulnerable or outdated backup software and misconfigurations that could allow unauthorized access.
- **Cloud infrastructures:** Scan for misconfigured storage areas (e.g., open S3 buckets), outdated images, or insecure access controls.
- **Container environments:** Detect vulnerabilities in container images or outdated base images that may result from known vulnerabilities.
- **E-mail systems:** Check for missing safeguards such as missing SPF, DKIM, or DMARC, as well as known vulnerabilities in used mail servers.
- **Network devices**: Finding outdated firmware versions or insecure default configurations.
- **Servers and clients**: Detect missing patches, insecure configurations, or known exploits.

Automated vulnerability scans are well suited for standard components. However, they can only detect vulnerabilities in (web applications) to a very limited extent, as these were often developed individually (individual software).

Penetration Testing

There is no "one" penetration test per se, as penetration tests are intended to simulate a real attacker. The penetration tests are therefore individual tests that are particularly useful for tests of business-critical (web) applications.
Penetration tests show the resilience of systems and applications against targeted attacks. More detailed information on penetration tests is described in the TeleTrusT "Penetration Tests" guidance document. Their release is planned for 2025.

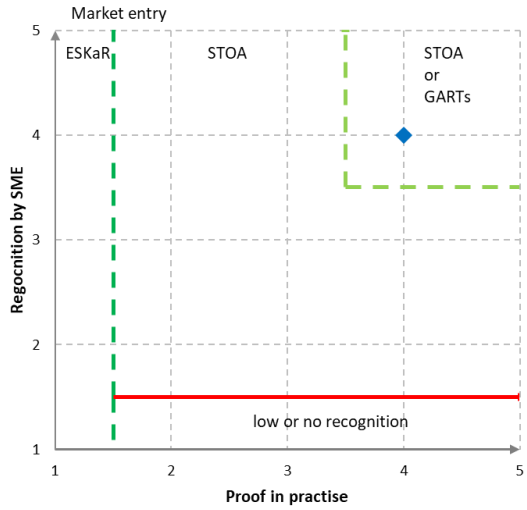
What protection goals are covered by the measure?

☒ Availability

☐ Integrity

☐ Confidentiality

Classification of the measure



4 Appendix

While the measures described above focus on the regulatory requirements in connection with information security, most of them remain only gray theory, because they are deliberately separated from business practice to explain the technology and classify it at the technology level according to the initially explained evaluation criteria.

This section is intended to establish the connection between the security measures described above and the changing security situation in the market. In this way, the practical relevance is to be worked out and the applicability of the measures is to be brought closer to the reader,

4.1 Measures against ransomware attacks

Ransomware describes a type of attack that blocks access to personal and corporate data (usually through encryption) and demands a ransom to release that data. In most cases, reconstruction of the original data is not possible without paying the ransom. Often, a ransomware attack is associated with the threat of publishing sensitive or secret data of the attack victim in order to substantiate the ransom demand. Other broad terms for ransomware include "*extortion/crypto trojans*" or "*extortion software.*"

The threat of ransomware has risen steadily in recent years and is one of the biggest threats facing both individuals and businesses.

In public, there is often talk of a ransomware attack. However, the procedure of such an attack is more complex and begins much earlier than is apparent at first glance. Each ransomware attack differs in individual steps, but the general approach is similar.

To counter the complexity of a ransomware attack, the use of just one measure (e.g. antivirus software or proxy filters) is insufficient. Several measures must be implemented at the same time and thus several lines of defense must be established. Examples of such activities include the detection of compromised accounts and weak passwords, the use of MFA, intrusion detection systems, etc.

In the following graphic, we show the individual steps and the corresponding protective measures that should be used depending on the respective steps:

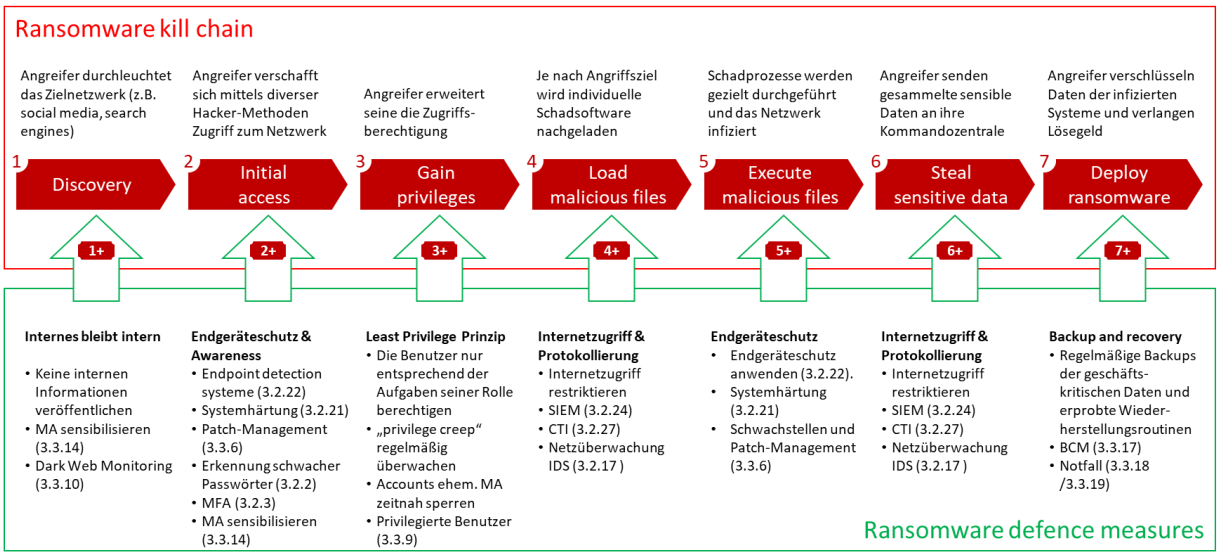


Figure 7: Ransomware kill chain and protections (example)

The possible steps and protective measures are briefly explained in the following table:

Ransomware-kill-chain (example)	Ransomware Security Measures
1) **Discovery** Attackers collect as much information as possible about the company being attacked, for example in public search engines (Shodan, Censys) or social networks.	1+) **Internal matters remain internal** Not to publish information that is only intended for internal purposes (network maps, IP addresses, organizational charts, contact details, etc.). As a possible approach, a classification of documents and data (public, internal, secret) can be made. Employees should also be trained in this (3.3.14 HR SdT). Dark Web Monitoring (3.3.10 HR SdT) can help to understand the current attack vectors.
2) **Initial access** Attackers gain access to the network using various hacker methods. An initial infection often occurs through phishing emails or malicious websites. At this point, the actual malicious code is not yet loaded.	2+) **Endpoint Protection & Awareness** Implement endpoint protection measures (3.2.22 HR SdT). Sensitize employees through regular awareness training (3.3.14 HR SdT). Disable macro execution or restrict it to signed macros only. Use measures to detect compromised accounts and weak passwords (3.2.2 HR SdT). If possible, use MFA (3.2.3 HR SdT). But also, other measures, such as server hardening (3.2.21 HR SdT) as well as vulnerabilities and patch management (3.3.6 HR SdT)
3) **Gain privileges** Attackers increase the privileges with which they act in order to achieve more far-reaching actions and thus a higher damage potential.	3+) **Least Privilege Principle** (PoLP) Ensure that users are only given the access rights they need to perform their tasks. Regularly check the privilege model for privilege creep. Align measures with the "user account cycle" and block accounts of former employees at short notice. Protect privileged accounts with MFA (3.2.3 HR SdT / 3.3.9 HR SdT).
4) **Load malicious files** The dropper now loads the actual malicious code ("payload"). This payload is often individually programmed and is not detected by antivirus software.	4+) **Internet Access & Logging** Allow Internet access to shared sites, block others. Depending on the need for protection, the use of ReCoBS (3.2.23 HR SdT) may be useful. Other technical measures such as SIEM (3.2.24 HR SdT) or CTI (3.2.27 HR SdT) as well as network monitoring using IDS (3.2.17 HR SdT) can support logging and monitoring.
5) **Execute malicious files** Further malicious code is downloaded, the attackers spread through the network ("lateral movement")	5+) **Endpoint Protection** Apply measures for endpoint protection (3.2.22 HR SdT). Implement other measures, such as system hardening (3.2.21 HR SdT) as well as vulnerabilities and patch management (3.3.6 HR SdT).
6) **Steal sensitive data** Sensitive data such as access data is sent to the attackers' command center ("command-and-control" server).	6+) **Internet Access & Logging** Allow Internet access to shared sites, block others. Depending on the need for protection, the use of ReCoBS (3.2.23 HR SdT) may be useful. Other technical measures such as SIEM (3.2.24 HR SdT) or CTI (3.2.27 HR SdT) as well as network monitoring using IDS (3.2.17 HR SdT) can support logging and monitoring.
7) **Deploy ransomware** The actual malicious code used to encrypt the data is executed.	7+) **Backup and recovery** In the event of a successful attack, of course, many measures must first be taken to find and close the infection vector and to limit the damage. To rebuild the systems and restore the data at a later date, up-to-date, non-infected backups are required. Further supplementary measures result from the BCM (3.3.17 HR SdT) and the preparations for an emergency (3.3.18 and 3.3.19 HR SdT)

Table 8: Measures against ransomware attacks

4.2 Classification of measures in ISO/IEC 27001:2022

The ISO/IEC 27001:2022 standard is an internationally recognized framework for information security management (ISMS). It supports organizations of all sizes and industries in systematically identifying, assessing, and addressing their information security risks. The standard is based on a risk-based approach and includes six key functions:

1. Context of the organization: The organization must identify internal and external influencing factors that affect the ISMS. This includes legal requirements, business goals, and stakeholder expectations.
2. Leadership: The top management is responsible for information security. It must define a clear security strategy, allocate resources, and ensure that security goals align with the corporate strategy.
3. Planning: Organizations must assess security risks and define appropriate measures to address risks. This also includes the definition of safety goals and their continuous review.
4. Support: The necessary resources, competencies and communication measures must be ensured in order to effectively operate and maintain the ISMS.
5. Operation: Security measures must be implemented and managed. This also includes the management of incidents and the continuous monitoring of the security situation.
6. Performance evaluation & improvement: Regular reviews through internal audits and management reviews are required to ensure the effectiveness of the ISMS and to continuously improve it.

In addition to these core aspects, ISO/IEC 27001:2022 emphasizes the importance of a continuous improvement process. This ensures that organizations can respond to changing threats and business needs.

An essential part of ISO/IEC 27001:2022 is Annex A, which contains a structured list of security measures (controls). These measures are closely linked to the ISO/IEC 27002:2022 standard, which provides detailed information on the implementation of these controls. The Controls are organized into four main themes: Organizational, Personal, Physical, and Technological Measures. They cover key security aspects such as access controls, encryption, incident management, and supply chain security. Companies use this appendix as a reference to select security measures and adapt them to their specific risks.

A key advantage of ISO/IEC 27001:2022 is the possibility of certification. Organizations can have their information security management system (ISMS) audited by an independent certification body to demonstrate compliance with the standard. The certification serves as an internationally recognized seal of approval and signals to customers, partners and regulators that the organization has implemented systematic and effective measures to protect information. This can not only increase trust in IT security, but also create competitive advantage by helping companies meet regulatory requirements and unlock new business opportunities.

Chapter Name	**Chapter #**	**ISO/IEC 27001:2022 Mapping**				
		Chapters 4-10	A.5	A.6	A.7	A.8
Authentication	3.2.1		A.5.15 A.5.16 A.5.17 A.5.18			
Assess and enforce strong passwords	3.2.2		A.5.17			
Multi-factor authentication	3.2.3		A.5.17			
Cryptographic methods	3.2.4					A.8.24
Encryption of hard drives	3.2.5					A.8.1 A.8.24
Encryption of files and folders	3.2.6					A.8.24
Encryption of emails	3.2.7					A.8.24

Chapter Name	Chapter #	ISO/IEC 27001:2022 Mapping				
Protecting electronic traffic with PKI	3.2.8					A.8.24 A.8.27
Use of encrypted VPN solutions (Layer 3)	3.2.9					A.8.21 A.8.24
Encryption (Layer 2)	3.2.10					A.8.21 A.8.24
Secure cloud-based data exchange services	3.2.11		A.5.23			
Data storage in the cloud	3.2.12		A.5.23			
Mobile voice and data protection	3.2.13					A.8.21 A.8.24
Protection of communication via instant messenger	3.2.14					A.8.21 A.8.24
Mobile Device Protection	3.2.15					A.8.1
Router Security	3.2.16					A.8.8 A.8.9
Network monitoring using an intrusion detection system	3.2.17					A.8.7 A.8.15
Web traffic protection	3.2.18					A.8.21 A.8.23
Web Application Protection	3.2.19					A.8.23
Protecting Remote Access to Networks	3.2.20			A.6.7		A.8.20 A.8.22
System hardening	3.2.21					A.8.9
Endpoint Detection & Response Platform	3.2.22		A.5.24 A.5.25 A.5.26			
Web isolation of Internet usage	3.2.23					A.8.22
Intrusion Detection and Evaluation (SIEM)	3.2.24		A.5.24 A.5.25 A.5.26			
Confidential data processing	3.2.25		A.5.12 A.5.23			A.8.2 A.8.5
Sandboxing for malicious code analysis	3.2.26		A.5.28			
Cyber Threat Intelligence	3.2.27		A.5.7			
Securing administrative IT systems	3.2.28					A.8.2
Directory Service Monitoring and Identity-Based Segmentation	3.2.29		A.5.18			A.8.15
Network segmentation and separation	3.2.30					A.8.22
Cloud Security Platform	3.2.31		A.5.23			
Tokenization	3.2.32					A.8.11
VOIP encryption with SIPS/SRTP	3.2.33					A.8.21 A.8.24
Encryption on Layer 1	3.2.34					A.8.24
Standards and norms	3.3.1					
Security organization	3.3.2	5.3				

Chapter Name	Chapter #	ISO/IEC 27001:2022 Mapping				
Information Security Management System (ISMS)	3.3.3	4 - 10				
Secure software development	3.3.4					A.8.25 A.8.26 A.8.27 A.8.28 A.8.29 A.8.30 A.8.31
Process Certification	3.3.5					
Vulnerability and patch management	3.3.6					A.8.8
Risk management	3.3.7	6, 8				
Personal Certification	3.3.8	7.2	A.6.3			
Securing privileged user accounts	3.3.9					A.8.2
Dark Web Monitoring	3.3.10		A.5.7			
Dealing with service providers	3.3.11		A.5.19 A.5.20 A.5.21 A.5.22			
Software Bill of Materials (SBOM)	3.3.12		A.5.9 A.5.21			A.8.8
Geo-redundancies	3.3.13					A.8.14
Raising user awareness	3.3.14	7.3	A.6.3			
IT Asset Management	3.3.15		A.5.9 A.5.10 A.5.12			
Incident Management	3.3.16		A.5.24 A.5.25 A.5.26			
Business Continuity Management (BCM)	3.3.17		A.5.29 A.5.30			
Emergency and crisis management	3.3.18		A.5.30			
Emergency drills	3.3.19		A.5.29 A.5.30			
Technical system audits	3.3.20					A.8.8

Table 9: Classification of measures in ISO/IEC 27001:2022

4.3 Classification of the measures in the NIST framework

The NIST Cybersecurity Framework was developed in the U.S. to help organizations across all industries manage their information and cybersecurity risks. It offers a flexible and repeatable approach based on existing standards and guidelines and includes five basic functions:

1. Identify: Understand and establish the organizational context, systems, assets, data, and capabilities that need to be protected. Manage assets that align with business importance.
2. Protect: Establish the appropriate protective measures to ensure that critical services are maintained even in the event of an incident.

3. Detect: Develop and implement the necessary measures for the early detection of cybersecurity incidents
4. Respond: Define actions and plans to effectively respond to detected cybersecurity incidents.
5. Recover: Planning for recovery from a cybersecurity incident and actions to restore normal business operations.

In addition to the five previously mentioned functions, "Govern" is considered an additional part of the NIST Cybersecurity Framework. The Govern feature plays a central role in the overall cybersecurity process and is reflected in various aspects of the framework.

6. Govern: The organization's cybersecurity risk management strategy, expectations, and policies are determined, communicated, and monitored.

Many companies use the NIST Framework as a reference to verify and optimize their own security measures. The framework also promotes communication about cybersecurity risks between internal and external stakeholders through the use of a common language. It is designed to be applicable to organizations with low cybersecurity maturity as well as those with advanced programs.

This guidance document takes on an intermediary role in order to explain the security measures and their characteristics to the application companies in a comprehensible way. To this end, it is useful to establish the measures described in relation to the current frameworks.

Chapter Name	Chapter #	NIST Assignment					
		Govern	Identify	Protect	Detect	Respond	Recover
Technical measures	3.2						
Authentication	3.2.1		X	X			
Assess and enforce strong passwords	3.2.2	X		X			
Multi-factor authentication	3.2.3			X			
Cryptographic methods	3.2.4			X			
Encryption of hard drives	3.2.5			X			
Encryption of files and folders	3.2.6			X			
Encryption of emails	3.2.7			X			
Securing electronic data traffic with PKI	3.2.8			X			
Use of encrypted VPN solutions (Layer 3)	3.2.9			X			
Encryption (Layer 2)	3.2.10			X			
Cloud-based data exchange	3.2.11			X			
Data storage in the cloud	3.2.12			X			
Mobile voice and data protection	3.2.13			X			
Protection of communication via instant messenger	3.2.14	X		X		X	
Mobile Device Protection	3.2.15	X		X			
Router Security	3.2.16			X			
Network monitoring using an intrusion detection system	3.2.17				X		
Web traffic protection	3.2.18			X			
Web Application Protection	3.2.19			X			
Protecting Remote Access to Networks	3.2.20			X			
System hardening	3.2.21			X			
Endpoint Detection & Response Platform	3.2.22				X	X	X
Web isolation of Internet usage	3.2.23			X			
Intrusion Detection and Evaluation (SIEM)	3.2.24				X	X	X
Confidential data processing	3.2.25	X		X			
Sandboxing for malicious code analysis	3.2.26				X		
Cyber Threat Intelligence	3.2.27				X		
Securing administrative IT systems	3.2.28			X			
Directory Service Monitoring and Identity-Based Segmentation	3.2.29		X		X		
Network segmentation and separation	3.2.30			X			
Cloud Security Platform	3.2.31			X			
Tokenization	3.2.32			X			
VOIP encryption with SIPS/SRTP	3.2.33			X			
Encryption (Layer 1)	3.2.34			X			
Organizational measures	**3.3**						
Standards and norms	3.3.1	X					
Security organization	3.3.2	X					

Chapter Name	Chapter #	NIST Assignment					
		Govern	Identify	Protect	Detect	Respond	Recover
Information Security Management System (ISMS)	3.3.3			X			
Secure software development	3.3.4			X			
Process Certification	3.3.5	X		X			
Vulnerability and patch management	3.3.6		X	X			
Risk management	3.3.7	X		X			
Personal Certification	3.3.8	X		X			
Securing privileged user accounts	3.3.9		X	X			
Dark Web Monitoring	3.3.10				X	X	
Dealing with service providers	3.3.11	X			X		
Software Bill of Materials (SBOM)	3.3.12		X	X			
Geo-redundancies	3.3.13			X			
Raising user awareness	3.3.14	X					
IT Asset Management	3.3.15		X				
Incident Management	3.3.16				X	X	X
Business Continuity Management (BCM)	3.3.17					X	X
Emergency and crisis management	3.3.18				X	X	X
Emergency drills	3.3.19				X	X	X
Technical system audits	3.3.20	X	X	X			

Table 10: Classification of the measures in the NIST framework

4.4 Impact of AI on Information Security

The term artificial intelligence encompasses several areas. Machine learning (ML), deep learning (DL) and generative AI (GenAI) are of greater importance in the context of IT security. Deep learning is a subset of machine learning (with multi-layered neural networks), while generative AI is a special case of deep learning.

What the three AI areas have in common is that all AI models can independently recognize patterns in large amounts of data after the training process. However, while machine learning and deep learning models tend to classify and categorize these amounts of data, generative AI models generate new content based on the patterns and statistical assumptions found.

The increasing integration of artificial intelligence (AI) into business processes is changing the landscape of information security, bringing with it both positive opportunities and significant security risks. On the one hand, AI can detect patterns and anomalies that indicate potential threats. On the other hand, the same technology can be used by attackers to find information about potential victims, carry out personalized attacks, or develop malware. Attacks on AI applications themselves are also possible, for example to actively influence their behavior.

AI to improve information security

One of the main benefits of AI is the ability to identify anomalies and unusual activity in large amounts of data. In contrast to traditional security technologies, where detection is usually based on matching patterns and signatures from previous attacks, AI is thus able to detect previously unknown threats.

AI also makes it possible to process and correlate data from many different data sources in a reasonable amount of time. AI and big data algorithms uncover connections that would often have gone unnoticed by a human observer.

Another benefit for businesses is the increase in efficiency that can be achieved by using AI in security technologies. AI systems conserve human resources by allowing security analysts to focus on relevant activities that have been detected as unusual. In addition, potential threats can usually be detected more quickly, which can significantly reduce the response time to security incidents.

AI as a tool for attackers

Attacker groups are also taking advantage of the capabilities of AI and using them specifically for their own purposes. This ranges from social engineering attacks to automated malware development. A great strength of AI lies in the efficient processing and analysis of publicly available information. Attackers use this functionality to collect and aggregate data about potential victims. The information collected subsequently forms the basis for tailor-made attacks. For example, personalized phishing emails can be created that are tailored to the respective target group. While traditional phishing messages are often conspicuous by spelling mistakes or poor translation, AI-generated messages are often almost indistinguishable from legitimate ones. At the same time, the sending of phishing messages can be highly automated, which can significantly increase the success rates of attackers.

In addition, AI can significantly lower the barrier to entry in the creation of malware for attackers. Malware can be generated using AI models that have been trained specifically for this purpose.

AI systems themselves can also become the target of attacks, both in the course of the training phase and during operation. In the so-called model inversion, attackers try to infer the underlying architecture with the help of the output of the AI and extract further information. The theft of a trained AI model can also have far-reaching consequences for a company. The OWASP Foundation maintains a list of AI-related risks, including risk factors and countermeasures.[46]

Protective measures against AI-related risks

Since AI is finding its way into almost all companies in various forms, appropriate protective measures are necessary to protect against AI-related risks. From a security perspective, machine and deep learning on the one hand and generative AI on the other have different effects. While the first two derive their *outputs* directly from machine-readable data sets (*inputs*), generative AI often generates outputs interactively in response to human input. This direct user interaction coupled with a high level of market dynamics and some AI peculiarities open up new attack surfaces, especially in the field of generative AI. In the machine and deep learning sector, on the other hand, the risks are more in the area of AI model security and the establishment of a secure development and test environment.

Before developing and deploying AI applications, applicable legal requirements must be identified. If products or services are offered on the basis of AI, the EU AI Act, which contains regulations for the use of AI, applies. The provisions of the GDPR must also be complied with. When using AI applications, for example, it must be checked whether the data entered is transmitted to the manufacturer of the AI application or to other third parties in order to prevent personal or sensitive data from being passed on without authorization.

The table below lists currently known security risks of AI models and appropriate preventive measures. Security-focused organizations like OWASP are constantly monitoring this space. OWASP not only provides annual lists of the ten most common attack methods[47] against generative AI models as well as checklists for AI security[48]. The organization also mentions concrete measures[49] to achieve safe and risk-free use of AI in companies. It distinguishes between:

- General security checks
  - Integrate AI into enterprise security programs
  - Measures for data control and data security
  - Measures to curb undesirable behavior of AI
- Measures for the use of AI
  - General usage monitoring
  - Measures against evasion attacks
  - Measures against Prompt Injection
  - Measures against the loss of sensitive training data
  - Measures against AI model theft
  - Measures against misbehavior of AI models

[46] https://owasp.org/www-project-machine-learning-security-top-10/
[47] https://genai.owasp.org/llm-top-10/
[48] https://genai.owasp.org/resource/llm-applications-cybersecurity-and-governance-checklist-english/
[49] https://owaspai.org/docs/ai_security_overview/

- Measures against threats at development time
  - General protection of development environment and supply chains
  - Measures against model poisoning
  - Measures against data leaks
- Measures against threats at model runtime
  - Protection against classic security risks
  - Measures against model manipulation at runtime
  - Measures against model theft at runtime
  - Confident handling of insecure model outputs
  - Measures against the entry of sensitive data

Not all threat scenarios are AI-specific. AI applications are often also classic SaaS applications and are subject to the associated security risks. Securing the development environment, but also the application API, for example, generally applies to all software projects. The following table provides an overview of AI security risks, protective measures and responsibilities for countermeasures.

	Secure Software Development Lifecycle	Code Review	Monitoring of adverse inputs	EDR/XDR	Audits of models against adverse inputs and trig-	Data Loss Prevention	Cleaning of training data	Security Audits	User training	User Authentication	Access control	Audit logs	Contracts	No Internet access for models	Bias detection software	Explainable AI Frameworks	Individual fact-checking	Reinforcement learning with humans in a loop and fine-tuning of the models	Legal requirements
Model poisoning – attackers falsify data in training	A	A		A	B		A	A			A	A				A			
Attackers steal or replicate the model	A		N	B		B		B		B	B	B							
Attackers steal or replicate confi- dential company data that is in the model	A	A	N	A	B	B	A	B		B	B	B							
Manufacturers trigger backdoors on certain topics / via dependencies		N		N				N				N		N					
Manufacturers deliberately incor- porate false state- ments into mod- els		N			N				N	N		N			N	N	N		
Model sends cus- tomer data to manufacturer		N				N		N	N	N	N	N	N	N		N			N
Copyright In- fringement							A		A				B			N		A	A

	Secure Software Development Lifecycle	Code Review	Monitoring of adverse inputs	EDR/XDR	Audits of models against adverse inputs and trig-	Data Loss Prevention	Cleaning of training data	Security Audits	User training	User Authentication	Access control	Audit logs	Contracts	No Internet access for models	Bias detection software	Explainable AI Frameworks	Individual fact-checking	Reinforcement learning with humans in a loop and fine-tuning of the models	Legal requirements
Vendor compromise due to application vulnerabilities	A	B		B		N		B			B	B	B	N					A
Disclosure of the system prompt through prompt injection			A		A	A		A		A	A	A	A	B					A
Compromise through supply chain attacks	B	B		B		N		B			B	B	B	N					B
AI manufacturers or AI providers legally or illegally collect user input						N			N	N	N		B	N					A
AI components in local software collect customer data		N		N		N		N			N	N	B	N					A
Vendors manipulate the outputs of the AI model					N				N				B		N	N	N		B
Models hallucinate and confabulate							A		N							N	N	A	
Models reproduce biases in their responses															B	B	N	A	A
Third-party attacks via compromised websites, emails, and phishing			N	N		N		N	N		N	N		B		B			
Users test Prompt Injections			B		B				N	N	N	B	B					A	A
Generate phishing emails			B						N	B		B	B					A	N
Retrieving illegal or harmful information			B		B					B		B	B		B	A	N	A	A
Fraud and manipulation with			B						N	B		B	B					A	N

	Secure Software Development Lifecycle	Code Review	Monitoring of adverse inputs	EDR/XDR	Audits of models against adverse inputs and trig-	Data Loss Prevention	Cleaning of training data	Security Audits	User training	User Authentication	Access control	Audit logs	Contracts	No Internet access for models	Bias detection software	Explainable AI Frameworks	Individual fact-checking	Reinforcement learning with humans in a loop and fine-tuning of the models	Legal requirements
machine-generated texts and images																			
Companies or third parties indirectly receive false information from AI users									N				N				N		
Reception of unreviewed AI content via social media, research literature, etc.									N				N				N		
Publications with implicit and unmentioned AI support									N				N				N		N

Table 11: Security risks of AI models and protective measures
Legend:

A = Countermeasures on the part of developers and/or vendors of the model
N = Countermeasures on the part of the users of the model
B = Countermeasures on both sides

The EU agency ENISA lists "misuse of AI for cyberattacks" among the top cybersecurity threats by 2030[50]. AI algorithms and tools that use them are constantly evolving. Attackers are benefiting from this development – attacks are becoming increasingly complex and more difficult for detection tools to detect. Companies, authorities and organizations are therefore faced with the challenge of optimizing the detection and defense of attacks with the help of AI and making it increasingly effective. The introduction and integration of AI must be carefully and quickly planned, continuously monitored, regularly updated and further developed.

In addition, staff training and raising awareness of the threats posed by AI is also essential. With AI becoming increasingly integrated into a wide range of business processes, a fundamental understanding of technology, as well as appropriate regulations and security measures, is necessary.

[50] https://ec.europa.eu/newsroom/ECCC/items/766303/en

4.5 Securing the supply chain

The resilience of supply chains is increasingly becoming a central, cross-industry requirement for companies. Due to geopolitical tensions, cyber threats and regulatory tightening, there is growing pressure to assess dependencies not only economically but also in terms of security. With the new NIS2 Directive, the updated ISO/IEC 27001:2022 and the German Supply Chain Due Diligence Act (LkSG), specific requirements come into force that affect both organizations and their service providers and suppliers. In addition, ISO 28000 provides a specialized framework for the structured assessment of safety-relevant aspects within the entire supply chain.

A key feature of NIS2[51] is its expanded focus on upstream service providers and suppliers. Companies will be obliged to explain how they identify, assess and control risks from their supply chain. This includes the ability to report incidents, as well as the right to audit security measures with third parties.

ISO/IEC 27001[52] in its revised version of 2022 is suitable for implementation. The standard requires systematic information security management that does not end at the company's boundaries. The new measures A.5.22 and A.5.23 specifically call for security in the supply chain to be managed and clear control mechanisms to be established at ICT service providers.

Another legal component is the German Supply Chain Due Diligence Act (LkSG), which has been binding for companies with more than 1,000 employees since January 1, 2023. It obliges companies to carry out systematic risk analysis along their global supply chains. Companies should not only evaluate their direct business partners but also take responsibility for upstream stages of the supply chain. In addition to human and environmental risks, IT security risks are also becoming increasingly important. A successful cyber-attack on a critical supplier can not only cause operational damage, but also have legal consequences – for example, if due diligence obligations are violated by interrupting the supply relationship.

ISO 28000 complements this approach in a meaningful way, as it focuses specifically on safety aspects in logistics processes. Unlike ISO 27001, which primarily addresses information security, ISO 28000 also covers physical risks, sabotage, product manipulation and safety-critical interruptions in transport and storage. The standard is particularly suitable for global companies or for organizations with increased risk in the physical supply chain. Through their structured approach, processes can be identified, evaluated and improved in order to make the entire value chain safer. From a practical point of view, it is advisable to use existing (information security) management systems and expand them in a targeted manner.

The integration of the requirements of NIS2, ISO/IEC 27001, ISO 28000 and LkSG is possible – and also sensible.

Decisive success factors are the involvement of suppliers in existing security processes and transparent communication about expectations and measures. In this way, meeting the increasing legal requirements can be used as a strategic advantage.

First of all, an overview of the supplier landscape must be created. This must make it clear which suppliers are connected to their own company and how. This does not only apply to suppliers of software products, but to all suppliers of the company, provided that they are connected to the company via direct or indirect technical or procedural interfaces.

Existing contracts should be reviewed, responsibilities redefined, and risk assessments regularly adjusted. In the case of strategically critical suppliers, it makes sense to carry out regular supplier audits in which the security aspects are also considered.[53]

Risk analysis enables the identification of critical processes, the determination of dependencies, the assessment of risks in connection with the respective threat situation and is thus also the basis for the identification of suitable security measures. On the technical side, access to company systems, the scope and sensitivity of processed data, the regional risk situation and the previous incident history are assessed, among other things.

[51] At the time of publication of this handout, the NIS2 had not yet been implemented in Germany.
[52] The automotive suppliers must implement the specifications according to the TISAX standard.
[53] See also chapter "Dealing with service providers"

Safety requirements must be defined for the risks identified. These have a dual purpose: on the one hand, they serve a structured identification of security measures for one's own company, and on the other hand, they support the dialogue with suppliers and create a common understanding of the necessary measures. Due to the strong interdependence of the processes, the security of the supply chain must be considered overall.

Modern supply chain management that wants to meet the requirements of NIS2, ISO 27001 and the LkSG requires an interplay of governance, processes and technology. Especially at the operational level, defined requirements must be translated into concrete safety measures in order to achieve actual effectiveness.

On a technical level, this means, for example, that access by external service providers is exclusively via secure, segmented connections. These include jump hosts with session recording, temporary access sharing, multi-factor authentication procedures, and logging of all activities. For particularly sensitive connections, SIEM systems should also be used to detect suspicious behavior in real time.

Various measures are required to ensure the security of the supply chain. The initial step begins with the procurement of IT security components. Under the keyword "Secure-By-Demand", the US Cybersecurity & Infrastructure Security Agency (CISA) has drawn up a guideline with 12 requirements for manufacturers to take into account in procurement.[54] This guide was primarily drawn up for the procurement of secure OT, but it can also be used in a slightly modified form for IT components. CISA emphasizes that the weighting of the individual recommendations should be adapted to the individual framework conditions. This applies in particular to the systems used or the available budget.

Especially in the case of software suppliers or software-heavy IT products, it is necessary to demand the provision of an SBOM[55] by the supplier and to keep it up to date on an ongoing basis. The SBOM is intended to make it possible to quickly identify and mitigate critical software content if necessary.

Vulnerability management also plays a role. External web services and interfaces should be regularly checked for configuration errors, outdated systems or insecure certificates by automated scans. For market-leading products and services, this information may be available for purchase. They are directly incorporated into the risk assessment.
At the data level, the consistent application of the principle of minimum rights allocation is essential. Service providers are only given access to what they absolutely need. In addition, all data flows must be encrypted, both in transit and at rest. Contracts should regulate this clearly and in a technically comprehensible way.

In addition to the technical security measures implemented, the continuity of business operations must always be considered. Emergency and restart plans must also[56] be prepared and tested.

Robust organizational structures are also needed: a supplier register with security profiles, audit cycles with risk-based intervals, coordinated escalation procedures in incident management, as well as training for all internal departments that work with third parties. Information security must be integrated into the everyday life of the purchasing, legal and project departments, as a natural part of corporate diligence. Securing the supply chain is not an isolated project, but part of a long-term security strategy. Companies that start implementing at an early stage and analyze their dependencies in a structured way not only create legal certainty, but also operational resilience and thus greater resilience in an increasingly unstable environment. This serves the interests of all stakeholders and increases the company's value in the long term.

[54] https://www.cisa.gov/resources-tools/resources/secure-demand-guide
[55] See chapter "Software Bill of Materials (SBOM)
[56] See chapter Emergency and Crisis Management

IT Security Association Germany (TeleTrusT)

The IT Security Association Germany (TeleTrusT) is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrusT embodies the largest competence network for IT security in Germany and Europe. TeleTrusT provides interdisciplinary fora for IT security experts and facilitates information exchange between vendors, users, researchers and authorities. TeleTrusT comments on technical, political and legal issues related to IT security and is organizer of events and conferences. TeleTrusT is a non-profit association, whose objective is to promote information security professionalism, raising awareness and best practices in all domains of information security. TeleTrusT is carrier of the "European Bridge CA" (EBCA; PKI network of trust), the IT expert certification schemes "TeleTrusT Information Security Professional" (T.I.S.P.) and "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) and provides the trust seals "IT Security made in Germany" and "IT Security made in EU". TeleTrusT is a member of the European Telecommunications Standards Institute (ETSI). The association is headquartered in Berlin, Germany.

Contact:

IT Security Association Germany (TeleTrusT)
Dr. Holger Muehlbauer
Managing Director
Chausseestrasse 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.