BSI Magazine 2024/01

Security in focus

In Focus:

Cyber Security

NIS 2 is Coming – What the BSI Offers for Companies

IT Security in Practice

Remote Work Will Remain Secure in the Future

Digital Society

Social Engineering: Protection against AI Supported Cyber Attacks

Federal Office
for Information Security

Editorial

Dear reader,

At the beginning of the year, the new National IT Situation Centre in Bonn was officially inaugurated. It is the heart of our IT security, where BSI specialists keep an eye on the cyber security situation in Germany around the clock. We have thus succeeded in creating the infrastructure we need to substantially improve cyber security in Germany. It is a first step towards a German cybernation.

„Building Cybernation Germany" is our response to the current threat situation: the security level of digitalisation in our country must be increased – in state institutions, in companies and, last but not least, for each and every individual person. Let's work together to ensure that Germany becomes cyberresilient!

How can we achieve this? By organising cyber security pragmatically and making it measurable. By using technological expertise in a more targeted way and also by strengthening the market for cyber security products and services. The goal is ambitious, but there is no alternative. After all, it's about the bigger picture: Germany must be and remain resilient in order to ward off cyber threats. At the same time, it must be ensured that citizens as well as companies and authorities can trust digital technologies.

As BSI, we are also committed to a strong digital consumer protection at an European level. In February, for example, we organised the first European symposium „Cybersecurity for Europe: Integrating the Consumer Perspective" in Dresden. The symposium brought together European cybersecurity organisations and proved to be a platform for networking, exchange and sharing knowledge.

In this issue, we also look back on the anniversary of our German IT Security Congress: For the 20th time, we brought together cyber security experts at the established forum to discuss IT security at the cutting edge. On the occasion of the anniversary, former BSI President Michael Hange reviews in an interview the early years of BSI, when East and West Germany were growing together in terms of protecting the IT infrastructure. IT-Grundschutz and CERT-Bund are also celebrating anniversaries this year – we have compiled these and many other exciting topics in the current issue of BSI Magazine.

I wish you a stimulating read!

Best regards

Claudia Plattner
President of the BSI

Tabel of Contents

Digital Consumer Protection: BSI Annual Review 2023 Published

To mark World Consumer Day on 15 March, the BSI has published its 2023 annual review in the field of digital consumer protection. Among other things, it takes a closer look at IT security incidents and trending topics with threat potential from 2023. For example, data leaks at companies and public institutions and phishing attacks on consumers were among the most common threats. At the same time, new trends such as the spread of artificial intelligence are creating a highly dynamic digital consumer market. These incidents highlight the urgent need to improve the protection and resilience of people's online activities. The thematic focus of the annual publication is therefore dedicated to "digital consumer resilience". The focus is on the question of what constitutes resilient consumers who are therefore better able to protect themselves against threats, react quickly in an emergency and minimise damage.

First Digital Ministers' Conference: Claudia Plattner Talks About AI

On the occasion of the first Digital Conference (DMK), which Federal Digital Minister Dr Volker Wissing and the digital leaders of the federal states on 19 April 2024 to successfully shape the digital transformation of the Federal Republic of Germany, BSI President Claudia Plattner spoke about the opportunities and risks of artificial intelligence. AI is a key technology of digitalisation and also has a wide range of potential uses for public administration. However, constantly new attack vectors on AI systems also require the ongoing development of countermeasures. Claudia Plattner praised the new digital conference: *"On behalf of the BSI, I would like to congratulate the newly founded DMK. We were very pleased to be here today, because it shows us that those responsible for digital issues at federal and state level are thinking about digitalisation and cybersecurity together. Also, and especially with regard to AI, it is crucial that we pool existing expertise and work together closely, consistently and uniformly. As the BSI, we would like to offer the federal states comprehensive advice on all aspects of IT security in connection with AI and make our information and tools available. We can already start sharing our experiences today – we are very happy to take advantage of this opportunity."*

Federal Minister for Digital Affairs Dr. Volker Wissing, HPI Managing Director Prof. Dr Ralf Herbrich, the digital directors of the federal states and BSI President Claudia Plattner

Berlin, 05.04.2024 From left: David Steinacker (GovTech Campus) and Thomas Caspers (BSI)

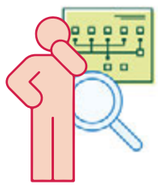
The Future of the Secure Cloud: BSI Joins GovTech Campus

The BSI has joined the GovTech Campus in Berlin. This promotes collaboration between administration, the technology scene, companies, science and civil society. Together with project partners, the BSI is working in a real-world cloud laboratory to make public cloud services securely usable for the federal administration and operators of critical infrastructures. This involves The aim is to systematically expand the public clouds of large cloud service providers from Germany and Europe and the so-called hyperscalers from the USA so that sensitive and classified data can also be securely stored and processed there. Thomas Caspers, Head of the BSI's Technology Competence Centres Divison, commented on the BSI's new commitment: *"Cloud computing is the backbone and driver of digitalisation in all areas, making cloud security indispensable for the resilience of modern information technology. To enable secure cloud use, the BSI provides technologically leading and immediately applicable solutions for the entire cloud operating spectrum. As a cybersecurity authority, our focus is on making digital sovereignty and critical infrastructures crisis-proof and future-proof at the same time."*

More than 60 IT service providers were trained to carry out the cyber risk check.

Successful Start: Training Courses on the CyberRiskCheck

To support small and medium-sized enterprises (SMEs) in increasing their cyber resilience, the Federal Office for Information Security (BSI) has developed the CyberRiskCheck together with partners. It offers SMEs standardised, needs-based advice from IT service providers. In April, more than 60 IT service providers came to Bonn for the first time to be trained to carry out the CyberRiskCheck. They can use the new expertise to help companies determine their own IT security level. BSI President Claudia Plattner: *"The CyberRiskCheck is a real win-win-win product: for small companies, for IT service providers and for the BSI. We have thus laid the foundation for an SME cybersecurity situation map, and this is an important step on the way to making Germany a cybernation. We are delighted that more than 120 additional IT service providers have already expressed their interest interest in carrying out the cyberRiskCheck."*



New for the Administration: BSI Support for Vulnerability Analysis of Administration Portals

In March, the BSI published the brochure "Getting started guide for the vulnerability analysis of administrative portals" for those responsible for digitalisation in the administration. The focus is on the secure provision of web portals as an interface to citizens. The high level of complexity harbours the risk of exploitable vulnerabilities in the administration portals, which could slow down digitalisation and cause lasting damage to trust in the administration. Vulnerability analyses are used to document both information security and compliance with legal requirements. Vulnerability analyses reduce the probability of a successful cyberattack and contribute to the secure digitalisation of the German administration.

Current Developments in the Field of Security & Artificial Intelligence

AI Is Booming: Implications for the Security and Transparency of AI Systems and the Cyber Threat Situation.

By Dr Matthias Heck, Head of Division Assessment Procedures and Technical Support of Digital Consumer Protection in Artificial Intelligence, and Dr Raphael Zimmer, Head of Division Artificial Intelligence and Security

Artificial intelligence (AI) has arrived in our everyday lives. This text discusses three key topics related to AI: the impact of misuse of AI on the cyber threat situation, the security of AI systems and the transparency of these systems.

AI helps us to work faster and more efficiently. However, it can also be misused: Criminal actors are already actively using artificial intelligence. For example, they can use AI programming assistants to develop and customise malware more quickly. AI can also help to identify vulnerabilities in programme codes.

AI also plays a major role in the distribution of malware in the context of social engineering. Attackers can use AI to strike more effectively, for example by creating personalised emails of convincing quality – with the aim of manipulating users into disclosing data, sending money or otherwise playing into the hands of criminals. Extracted data volumes can also be analysed more effectively in the event of attacks and sensitive content can be identified more quickly, for example in order to lend weight to blackmail attempts. If AI is used, this also lowers the requirements for the perpetrators, as hardly any prior technical knowledge is required for certain tasks.

An analysis by the British National Cyber Security Centre on the short-term effects of AI on the cyber threat situation almost certainly assumes that AI will lead to more and stronger cyber attacks in the next two years. It is therefore important that Germany quickly develops into a cybernation that actively implements cybersecurity in all areas.

Due to the increasing working speed of cyber criminals, resilient infrastructures with fast patching, detection and response capabilities are needed. Training and sensitisation of users will also become even more important. Due to the increasing dynamics, efforts on the defence side must be intensified.

INCREASING IMPORTANCE OF THE SECURITY OF AI SYSTEMS

After several years in which the security of AI systems was more of an academic research area, the topic is now very relevant due to the widespread use of AI systems in practice. In 2023, developers in particular examined how AI language models can be profitably integrated into their applications. We are now seeing that other target groups are also actively putting AI applications into practice: By providing chatbot construction kits, professional users without in-depth AI and IT knowledge can put together chatbots themselves on a modular basis. The role and behaviour of the chatbot can be determined using instructions (see Figure). Documents can be stored as a knowledge base for background information on products or a company. It is possible to grant the chatbot access to the Internet to retrieve real-time information and to control systems in the backend via function calls. In addition, the AI can create suitable images depending on the context and write and compile programme codes. Complex data analyses are also possible.

BSI PUBLICATION “GENERATIVE AI MODELS” HELPFUL

When configuring such a chatbot, there is a lot to consider from a security perspective. For example, stored documents or instructions can usually be extracted by users. This also applies if the chatbot has been explicitly instructed not to provide any information about these documents. Extensive sensitisation of users is therefore recommended before using such chatbot construction kits. The BSI publication “Generative AI models: opportunities and risks for authorities and industry”, which is regularly updated and supplemented by the BSI, is a good starting point.

Conceptual representation of a chatbot construction kit with various components

TRANSPARENCY IS ALSO IMPORTANT

From a scientific point of view, AI models or systems are transparent if they are self-explanatory. This applies to various algorithms, such as the decision tree. Here, the path of a prediction or statement made by the AI system can be traced without much effort. Unfortunately, algorithms behind new and modern AI systems, such as those found in large language models or generative AI applications, do not exhibit this transparency. On the contrary, they are often referred to as black box models: They are systems that do not allow insight. Although the input can be traced during the application, it is not possible to trace the decisions on the basis of which the system generates an output. However, as these systems are being used more and more in practice – for example in the automated summarisation of texts – the concept of transparency is also important for these systems.

EXPANSION OF THE CONCEPT OF TRANSPARENCY NECESSARY

It is therefore necessary to expand the concept of transparency in connection with AI systems. In the example of the chatbot described above, not only should it be made transparent how the output is generated, but the system‘s boundary conditions should also be described. For example, the models and training data used, the exact purpose and limitations of the systems, including possible risks and dangers, should be openly communicated, as should the physical location where the system is operated. It would also be important to clearly state how the data that users enter into the system is further utilised.

Transparent AI systems have two decisive advantages: they empower both the consumers who use the systems and third parties affected by their impact, and they sensitise developers to dangers and risks. ■

Information on short URLs and (speaking) document IDs can be found here:

https://www.ncsc.gov.uk/news/global-ransomware-threat-expected-to-rise-with-ai

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.pdf?__blob=publicationFile&v=5

www.bsi.bund.de/ki

Cybersafe? But Secure!

What Companies Can Do to Increase their Level of Cybersecurity Today and Prepare for the Implementation of the NIS-2-Directive in the Best Possible Way

By Katrin Kubica, Head of Division Cooperation with Manufacturers and Service Providers

Cybersecurity must be on the agenda: this year, the European NIS-2-Directive is a particular focus. Companies should take measures now at the latest to increase their level of cybersecurity. Irrespective of regulatory or legal requirements, the BSI has developed offers and assistance for this purpose.











> *"Whether today or on the basis of NIS 2: Companies should start planning the increase their level of cybersecurity to move forward. 100 per cent security does not exist, but every measure counts!"*
>
> Katrin Kubica, Head of the Cooperation Division with manufacturers and service providers

Member states are obliged to transpose the NIS-2-Directive (Network and Information Security Directive) into national law by October 2024 at the latest. This is an EU-wide regulation that obliges companies and institutions to improve their respective cyber and information security measures.

It is still unclear whether Germany will have adopted the so called "NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz" (NIS2UmsuCG) by autumn. What is certain, however, is that there is no alternative to increasing the level of IT security. This is a major challenge, especially for small and medium-sized enterprises (SMEs). The personnel, financial and structural hurdles are immense, while at the same time the pressure to act is increasing due to the growing threat situation. As everywhere, the most important step is to get started. Once a company has taken this step, it can work together with other companies and with the BSI as the federal cybersecurity authority to develop towards greater cybersecurity.

SERVICES OFFERED BY THE BSI

The BSI has been around for more than thirty years and has a wealth of experience in methods, recommendations and standards for greater cyber resilience in the economy. In addition to the BSI's self-help programmes, there are numerous opportunities for exchange and cooperation. You can find a detailed overview of the BSI's offerings for businesses on page 12.

OUTLOOK

The NIS2UmsuCG will have a huge impact on increasing the level of cybersecurity in Germany. Companies and institutions will be obliged to take a number of measures. The planned requirements and regulations are sensible and long overdue. In future, companies will have to take even more suitable, proportionate and effective technical and organisational measures to protect the IT and processes of the services they provide, avoid disruptions and minimise the impact of security incidents. These include mandatory training for management, measures to deal with IT security incidents, backup and crisis management and the use of multi-factor authentication.

Cybersecurity is not only a prerequisite for successful digitalisation, but also crucial for our coexistence, our economic strength and digital sovereignty. Let us see the implementation of the NIS-2-Directive as an important EU-wide regulatory framework and an important contribution to Germany as a cybernation. Because only with a uniformly high level of cybersecurity can we meet the growing challenges in IT security today and in the future. More cybersecurity is not optional. It is a prerequisite for success. The BSI provides support not only with the services mentioned above, but also beyond that. As soon as the NIS2UmsuCG has been adopted, the BSI will provide information on its implementation.

To this end, the BSI is developing the "NIS-2 Checker", which enables companies to quickly check whether they are affected by the EU's NIS-2-Directive by answering just a few questions. As soon as the directive has been implemented at national level, the NIS-2 Checker will also be updated. The "NIS-2 Checker" indicates all resulting obligations and offers assistance with implementation. ■

NIS 2 is Coming – What the BSI Offers Companies

Alliance for Cyber Security

Brief description:
With the Alliance for Cyber Security, founded in 2012, the BSI is pursuing the goal of strengthening the resilience of Germany as a business location against cyber attacks. The initiative is Europe's largest public-private partnership in the field of cybersecurity for more prevention in the economy.

Target group:
Companies of all sizes, associations, chambers of commerce, research

Das bietet die ACS Unternehmen:
- The expertise of the BSI and the ACS partners,
- trustworthy exchange of experience on topics such as attack vectors, suitable protective measures, tips on security management, incident handling, etc,
- exclusive and free partner offers for ACS participants to expand their cybersecurity expertise,
- Participation in expert circles, experience circles and the Cyber Security Days,
- regular up-to-date information and events on cybersecurity.

» **We currently recommend:** "Managing Cyber Risk – A Handbook for German Boards Directors"

Cyber Security Network

Brief description:
The Cyber Security Network (CSN) is a voluntary association of qualified experts for IT incident handling. The aim of the cyber-security network is to establish a nationwide decentralised structure that offers efficient and cost-effective support to SMEs and citizens in the event of IT security incidents.

Target group:
Companies and private individuals (SMEs and citizens)

What the CSN offers companies:
The CSN offers qualified IT incident handling experts who agree to provide their individual expertise to resolve IT security incidents. By taking on reactive activities, they help to identify and analyse IT security incidents, limit the extent of damage and avert further damage.

» **We currently recommend:** Digital rescue chain:

IT Grundschutz

Brief description:
With its modular concept, IT Grundschutz is an essential tool for increasing and continuously improving information security.

Target group:
Authorities and companies of all sizes

What IT-Grundschutz offers companies:
IT Grundshcutz offers a systematic approach that makes it possible to identify and implement the necessary security measures.

We currently recommend:
IT-Grundschutz profiles, which have developed specific fields of application for certain sectors, make implementation even easier. These profiles already exist for craft businesses, shipping companies, chemical companies, IT service providers and many others. Others, such as aviation security and IT security for supply chains, are currently being developed.

» http://www.bsi.bund.de/IT-Grundschutz

UP KRITIS

Brief description:
The UP KRITIS is an independent partnership between KRITIS operators, their associations and the relevant authorities on the topics of cyber and physical security. As a KRITIS operator, you can participate free of charge and without obligation, even if your organisation is below the thresholds of the BSI Criticality Ordinance.

Target group:
KRITIS operators, their associations and the competent authorities

What the UP KRITIS offers companies:
The UP KRITIS offers you many opportunities: You can network within your sector and across sectors. Together with other operators and the relevant government agencies, you can help to determine the state of the art in working groups or take part in crisis exercises, for example. You receive information on national and international legislative projects and can comment on them. You receive cyber-security alerts and management information and can report incidents yourself.

» **We currently recommend:**
The paper "Utilisation of cloud-based services in critical infrastructures – an aid from the UP KRITIS"

CyberRisikoCheck

Kurzbeschreibung:
The CyberRiskCheck enables small and medium-sized enterprises (SMEs) to determine their cybersecurity level using a simple, cost-effective and standardised procedure (DIN SPEC 27076).

Target group: Small and micro enterprises (< 50 employees), medium-sized companies

What the CyberRiskCheck offers companies:
After a one- to two-hour survey by an IT service provider, SMEs receive a detailed report describing any deficits and providing specific recommendations for action. The survey examines a total of 27 requirements in six subject areas. The recommendations for action are categorised according to urgency and also provide information on government support measures at federal, state and municipal level that the company can take advantage of.

» **We currently recommend:** Carry out a cyber risk check for your company as soon as possible. Further information and qualified service providers can be found at

Quantum Computers as an IT Risk

The BSI Study on the Current Threat Situation

By Dr Heike Hagemeier, BMI Division of International Cybersecurity and Cybersecurity Research, and Stephanie Reinhardt, BSI Division of Specifications and Development of Cryptographic Procedures

Quantum technologies offer enormous potential for overcoming previously unsolvable or complex problems. However, it is also true that the development of powerful quantum computers poses a threat to our IT security.

So far, there is no quantum computer that can execute cryptographically relevant algorithms. However, when the time comes, our confidential communication and security-relevant data will be at risk. Attackers are already storing encrypted information so that they can decrypt it as soon as the necessary technology is available ("store now, decrypt later").

The BSI has updated a study from 2017 to 2020 in the project "Ongoing update of the study on the state of development of quantum computers". The study serves to assess the development status of quantum computers that can potentially be used for cryptanalysis. It also looks at the relevance of selected quantum algorithms.

THE LATEST HARDWARE DEVELOPMENTS

The biggest challenge in the development of quantum computers is currently their susceptibility to errors. The correction of these errors is characterised by an enormous overhead – the logical qubits that describe an algorithm consist of a large number of components, the physical qubits. Although initial success has already been achieved in error correction, in most cases the hardware does not yet have the necessary quality to achieve an improvement by means of error correction. Many different quantum computer platforms are currently being researched and it is not yet clear which will prevail. A layered model for evaluating the platforms was developed for the study. It begins with the demonstration of basic functions and progress to the fault-tolerant implementation of algorithms. Significant progress has been made compared to the last version of the study, particularly with ion traps and superconducting qubits. The production of superconducting circuits is already technologically advanced and can be easily optimised. This leads to available quantum processors with more than 1,000 qubits. However, these qubits are still quite error-prone and not all of them can interact directly with each other – the so-called connectivity is low. In comparison, quantum computers based on ion traps can perform more precise computing operations and have higher connectivity. Before error-correcting quantum computers are available, "noisy intermediate-scale quantum (NISQ) technologies" are already in use. These do not correct errors, meaning that only a limited number of calculation steps can be carried out. The current version of the study is the first to consider algorithms designed for cryptanalysis with NISQ computers.

RELEVANCE OF QUANTUM COMPUTERS FOR CRYPTANALYSIS

Much of the public key cryptography used today is based on the factorisation or discrete logarithm problem. In the 1990s, Peter Shor showed for the first time that these two problems can be solved efficiently if a sufficiently powerful quantum computer is available. In order to be able to estimate when quantum computers will provide such an advantage in cryptanalysis, it is also necessary to precisely analyse the quantum algorithms themselves. An estimate by Gidney and Ekerå from 2021, for example, states that with 20 million physical qubits, the RSA-2048 scheme can be broken in eight hours. This is widely used on the internet, for example, to secure the confidentiality and authenticity of data.

Quantum computers also offer possibilities for analysing symmetric cryptography, such as Grover's search algorithm and Simon's algorithm. However, the effects are currently much less serious.

There is now also a wide range of heuristic algorithms that are specifically designed for use with NISQ computers. However, the scalability of none of these algorithms has yet been proven. This suggests a low cryptographic relevance of such algorithms and NISQ technologies. However, it is important to continue monitoring developments.

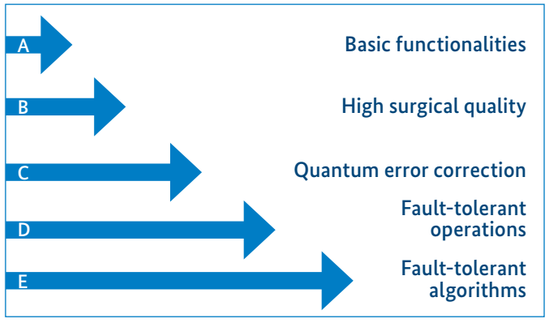


Figure 1: Layer model for the evaluation of quantum computing platforms

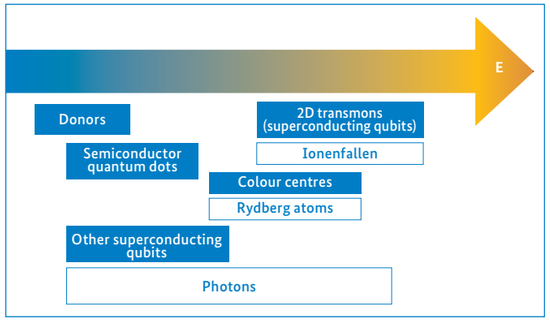


Figure 2: Categorisation of technologies according to their stage of development

CONCLUSION

The study shows that the development of quantum platforms and algorithms is making steady progress. As things currently stand, it is assumed that it will take at least a decade before cryptographic relevance is achieved. However, this period can be shortened at any time as soon as leaps in development take place. Current publications by various research groups suggest just such leaps, such as platforms based on neutral atoms. These and other publications will be taken into account in the next update of the study, which is planned for the end of this year. In order to mitigate the risk posed by potential, particularly drastic developments, the BSI is working under the assumption that a cryptographically relevant quantum computer will be available from the 2030s. Accordingly, the migration to quantum-safe cryptography is pushed forward. The focus here is particularly on protecting information that will still need to be confidential in a decade's time in order to prevent the "store now, decrypt later" scenario.

However, the goal must be a holistically quantum-secure cybernation in Germany. There is still a lot to do to achieve this! ■

The study and further information can be found at:

www.bsi.bund.de/Quanten

www.bsi.bund.de/qcstudie

Anchoring Cybersecurity and Digitalisation in Germany

With Its New Strategy, the BSI Shows a Way How the Cybernation Germany Can Be Achieved

The goal is ambitious, but there is no alternative. Because it is about the big picture. Germany must be and remain resilient in order to ward off cyber threats. At the same time, it must be ensured that citizens and companies alike can trust the digital technologies they use. This is why the BSI has developed a strategy on how Germany can become a cybernation: A country that has first-class mastery of cybersecurity and digitalisation.

What does a cybernation need? Citizens who are awake and alert. A society that is aware of the dangers of digital progress. People who do not stand like rabbits in front of a snake, but who look reality in the eye. People who can rely on the state to ensure that digitalisation is secure – but who are also able to protect their digital environment on their own. Initiatives to protect against cyber threats should be on the agenda. This is because ongoing digitalisation and increasing networking are increasing the attack s these are being exploited.

MASSIVE POLITICAL DISINFORMATION CAMPAIGNS

The BSI report on the state of IT security in Germany last year paints a worrying picture: a quarter of a million new malware variants and 21,000 infected systems every day, plus more than 2,000 vulnerabilities in software products per month. The damage caused by attacks on German companies totalled more than 200 billion euros. At the beginning of this year, the Federal Foreign Office registered increased attempts by foreign actors to influence domestic policy in Germany. Massive campaigns were used to influence debates on foreign policy issues in online networks. Russia was suspected of fuelling discontent against the German government coalition with more than 50,000 fake accounts on the online platform X and more than one million German-language tweets. The accusation frequently emerged that the German government was neglecting its own population in order to support Ukraine. Disinformation is used to destabilise democratic societies.

DECEPTIVELY REAL AI FAKES

People in the US were also alarmed when members of the Democratic Party received automated calls in which US President Joe Biden supposedly urged them to ignore the primaries. The deceptively real-sounding voice proves once again how powerful fakes using artificial intelligence (AI) are. Pop star Taylor Swift can also tell you a thing or two about it: AI-generated nude pictures of her brought the topic of cybercrime a great deal of attention worldwide.

TARGETED INTERFERENCE WITH SATELLITE NAVIGATION

Security experts in the Baltic Sea region are also paying particular attention, as they have been observing targeted disruptions to satellite navigation for months. According to the Federal Ministry of Transport, interference with the navigation signals emitted by the Global Positioning System (GPS) satellite navigation system has been reported from German airspace since December 2023. Russia is also suspected in this matter. Satellite navigation is used to determine one's own position and for route planning in vehicles. Aeroplanes and ships use satellite navigation. It is also relevant for automated processes in agriculture.

"The challenges in cybersecurity a country does not meet on paper, but through technology. To this end, Germany can rely on excellent technological expertise for the development of solutions. Digitalisation needs to be accelerated, to keep pace with the developments of our time!"

Claudia Plattner, President of the BSI

WHY THE AGE OF POLYCRISES CALLS FOR A CYBER STRATEGY

Geopolitical tensions, such as the threat of escalation in the Middle East conflict and the Russian war of aggression on Ukraine, global challenges, such as tackling climate change and securing energy supplies, as well as domestic issues, including the impact of the coronavirus pandemic, all have an impact on the cybersecurity situation. The world has always known multiple crises, but the age of polycrises has now begun: Critical situations can no longer be viewed in isolation from one another. Deepfakes on social media platforms are used to influence opinions, manipulate elections or destabilise societies. „We are all called upon to confront the dangers consistently and courageously," is therefore a core idea in the BSI's cyber strategy.

“With the ‚Cybernation Deutschland‘ initiative, we want to together to ensure that companies and operators of critical infrastructures become more resilient and arm themselves even more strongly against cyber attacks. Secure digitalisation is our common goal. After all, the stronger and more resilient we are as a business location in Germany, the more attractive we are for science, companies and IT and IT specialists. We also want to ensure greater awareness of cybersecurity throughout our society and improve digital consumer protection.”

Nancy Faeser, Federal Minister of the Interior and for Home Affairs

UTILISING EXPERTISE, ENABLING TECHNOLOGY

Every day, cyber criminals attack companies and institutions in Germany. The high level of professionalism in their approach is particularly worrying: State-of-the-art technology such as AI is being used and the division of labour continues to increase, especially in ransomware attacks and “cybercrime-as-a-service”, a perfidious type of criminal service. People in Germany are living more digitally than ever before. Nobody wants to do without online shopping or online banking, consuming news and information online or spending time on social media – so it is in everyone‘s interest that digital services are secure.

This is where the BSI comes in and strengthens the state, society and commercial enterprises in their initiatives to increase cyber resilience. A country does not meet the challenges of cybersecurity on paper, but through technology. Germany can draw on excellent technological expertise to develop solutions. Digitalisation must be accelerated in order to keep pace with the developments of our time!

CYBERSECURITY ONLY WORKS HAND IN HAND

The example of GPS disruptions illustrates the situation: satellite systems are indispensable for coping with increasing traffic density and automation in the mobility sector. Experts are analysing disruptions and learning from them for future technological developments. The Federal Network Agency, which is responsible for protecting the electromagnetic spectrum, is monitoring the situation and exchanging information with the federal and state authorities involved, the German Armed Forces and other users of airspace – because cybersecurity is a joint task.

JOINT ACTION STRENGTHENS RESILIENCE

Therefore, cooperation is a central keyword of the BSI cyber strategy: consistent co-operation between politics, business, science and society at both federal and state level is required so that Germany can make targeted use of its technological expertise and increase digital security. If Germany‘s self-image as a cybernation grows, the necessary resilience can be built up. The BSI sees itself in many roles in this process: as a driver and enabler, as a partner and helper, as an architect and at the same time as a supporting pillar in the country‘s security architecture. The BSI knows that the efficient and effective co-operation of all stakeholders and a functioning coordination of the necessary measures are mammoth tasks.

THE BSI CYBER STRATEGY AT A GLANCE

In order to make Germany a cybernation together, there are six important fields of action Graphic

The BSI acts as a promoter of cybersecurity. It endeavours to anchor the protection of critical systems and sensitive information in the awareness of all stakeholders. Decision-makers in Germany should be encouraged to put the topic on their agenda on a regular and recurring basis.

BSI ESTABLISHES SUSTAINABLE NETWORKS WITH STAKEHOLDERS

With whom is the BSI in dialogue? At federal level with authorities, organisations and companies that provide IT services for the federal government, for example in the area of networks or through applications for users. The BSI draws up specifications, provides advice, proposes specific implementations, reviews security requirements, promotes the use of secure technologies and coordinates directly effective measures to protect information technology. It also cooperates with the authorities at federal level that are involved in Germany's cybersecurity within their area of responsibility, for example in law enforcement, border controls, military cooperation, emergency response and civil defence.

At state level, the BSI is in contact with the stakeholders responsible for cybersecurity in all 16 federal states: These are state ministers, "Chief Information Security Officers" (CISO), "Computer Emergency Response Teams" (CERT), cross-state co-operatives with IT tasks as well as state agencies or other state institutions. The BSI supports cross-state initiatives with federal participation and, in individual cases – for example on the basis of a cooperation agreement – also states directly. At the municipal level, the BSI network includes municipal administrations and municipal umbrella organisations.

"The BSI team is taking on the mammoth task of substantially increasing the cyber resilience of companies and institutions by actively driving forward improvements – always aware that the challenges in cybersecurity cannot be met on paper, but that they require action."

Claudia Plattner, President of the BSI

In politics, all parliamentary players at federal and state level as well as organisations, initiatives, foundations and think tanks are among the partners. In addition, there are universities, scientific institutions, research organisations and individual scientists. They form the core of national and international BSI cooperation with the scientific community. Discussions take place at a professional and technical level, and findings are exchanged bilaterally and at specialist conferences. They learn from each other with the common goal of researching the fundamentals of cybersecurity and actively shaping further developments to make them marketable.

VIBRANT ECOSYSTEM FOR CYBERSECURITY PRODUCTS

The BSI team is taking on the mammoth task of substantially increasing the cyber resilience of companies and institutions by actively driving forward improvements – always in the knowledge that the challenges in cybersecurity cannot be met on paper, but that they require action. The BSI relies on the excellent technological expertise in Germany to develop solutions. Cybersecurity is a key success factor here: developing solutions increases the security and speed of digitalisation. A vibrant ecosystem for cybersecurity products and services is being created with support from three sides: politics, business and science. This means that Germany is prepared and can respond efficiently and effectively to further challenges.

PROGRESS THANKS TO THE BSI VALUE CHAIN

An important prerequisite for cybersecurity is the assessment of the security situation. Through research and testing at the BSI, necessary requirements are identified and solutions are tested for their viability. The BSI value chain is used to define requirements and specifications for secure products and services as well as for security in organisations. The BSI also provides implementation aids. Certifications are used to check whether products and services fulfil the security requirements. The BSI also assesses the security of the federal administration and critical infrastructures. The results of the assessments create transparency with regard to the security situation in Germany. With "Security Operations" and support, the BSI prepares for emergencies and crises.

THE VISION OF A CYBERNATION IN GERMANY

The BSI and its partners have long since started to implement the masterplan for cybersecurity.

THE FOLLOWING GOALS ARE AT THE CENTRE OF THE VISION:

Companies and institutions in Germany are resilient to cyber attacks.

Germany is well positioned against cyber espionage and sabotage.

German society recognises targeted external influence and knows how to deal with it.

People in Germwany move safely in cyberspace.

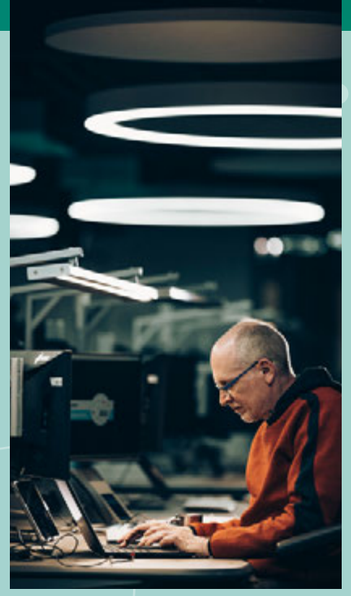
Germany is a pioneer of secure and efficient digitalisation.

People trust the digital services offered by the state.

Germany is an attractive and innovative location for digital technologies and services.

More information on Cybernation and the BSI's strategic goals can be found here:

https://www.bsi.bund.de/dok/cybernation-deutschland



Foundation of the Cybernation Germany

New National IT Situation Centre Keeps an Eye on Cybersecurity Around the Clock

By Sebastian Brück, Head of Division National IT Situation Centre, 24/7 Permanent Service, and Dr Christian Eibl, Head of Division Nation IT Situation Centre, Principles and Reporting Point

The new National IT Situation Centre is equipped with state-of-the-art communication technology and has ten workstations in regular operation, from which the BSI specialists keep an eye on the cybersecurity situation for Germany around the clock. At the opening in February 2024, Federal Minister of the Interior Nancy Faeser and BSI President Claudia Plattner launched the "Cybernation Deutschland" initiative.

The BSI's "Cybernation Deutschland" initiative aims to achieve a high level of digitalisation security in Germany – this applies to state institutions as well as to the economy and society. In addition to increasing cyber resilience, the initiative aims to create greater awareness of the topic of cybersecurity overall, to make cybersecurity pragmatic and measurable, to make more targeted use of technological expertise in Germany and to strengthen the market for cybersecurity products and services in Germany.

This approach is urgently needed, as companies and institutions in Germany are attacked by cyber criminals every day. Ransomware attacks currently pose the greatest threat. In addition, there is a growing professionalisation on the perpetrator side and an increasing number of security vulnerabilities.

In the new National IT Situation Centre, the BSI has state-of-the-art infrastructure at its disposal to substantially increase cybersecurity. The staff at the Situation Centre regularly exchange information and assessments on the cybersecurity situation with other experts at the BSI – keyword: "integrated value chain" – as well as with national and international partners.

ON DUTY AROUND THE CLOCK

The National IT Situation Centre monitors and evaluates cybersecurity incidents 24/7 and therefore has a reliable picture of the current IT security situation in Germany at all times. With this overview, the BSI experts can identify threatening situations such as waves of attacks or potentially exploitable vulnerabilities at an early stage and promptly and competently assess the need for action and options for action both at state level and in the economy. During normal office hours, BSI experts for critical infrastructures (KRITIS) and the Federal Computer Emergency Response Team (CERT-Bund) as well as the information security officers of the Cyber and Information Space Command (KdoCIR) support the National IT Situation Centre. Outside office hours, CERT-Bund and KRITIS are on call. Cooperation with the KdoCIR takes place via the established interfaces between the two authorities.

The National IT Situation Centre is also the BSI's central reporting office. Various statutory or contractually stipulated, but also voluntary reporting centres converge here. Every year, the IT Situation Centre receives around 2,800 reports via 22 reporting points. Active open source intelligence (media monitoring, social media analyses, etc.) and in-house sensors supplement the information base.

HOW THE BSI CONTROL CENTRE REACTS TO A CYBERSECURITY INCIDENT

How can you imagine everyday life in the BSI control centre? An example: A report of a security incident arrives and monitoring systems are activated at the same time. After immediate consultation with the person affected, everything points to malware. The following questions need to be answered: What is the aim of the software? What effects can be expected? Who else could become a victim and what does this mean for Germany's cybersecurity situation?

The broad expertise of the BSI is pooled in the National IT Situation Centre, from where the response of the federal cybersecurity authority is coordinated: IT specialists from a wide range of disciplines work together to analyse threats and develop countermeasures. As cyber threats do not stop at national borders, up-to-date information and assessments are also shared with national and international partners, such as our NATO partners, using established processes.

High-ranking visitors at the opening of the new National IT Situation Centre: Federal Minister of the Interior Nancy Faeser, BSI President Claudia Plattner and the Deputy Inspector of Cyber and Information Space (CIR), Major General Jürgen Setzer (from left to right). Sebastian Brück, Head of the Permanent Information Service, guided the guests through the new premises.

FROM THE IT SITUATION CENTRE TO THE SPECIALIST DEPARTMENTS

Once the initial response has been completed, the new findings are incorporated into the BSI's long-term work: Should the results be included in the IT baseline protection recommendations? Do technical guidelines and certification procedures need to be adapted? Do advisory processes need to be supplemented? With its continuous findings from situation monitoring and assessment, the National IT Situation Centre makes an important contribution to enabling the BSI to fulfil its role in shaping Germany's cybersecurity.

RECOGNISING THE SITUATION – AND REACTING APPROPRIATELY

While the findings flow directly into the protection of government networks, recommendations for action reach different target groups in a timely and targeted manner via suitable distribution mechanisms. These include warnings for the general public, suitable information for IT professionals in critical infrastructures, the federal administration and smaller companies to protect their systems and, last but not least, information for consumers. Depending on the threat situation and the extent to which they are affected, other players such as the Mobile Incident Response Team (MIRT) will also begin their work. Through an intensive exchange of information in the National Cyber Defence Centre, other authorities are also informed in good time and measures are coordinated.

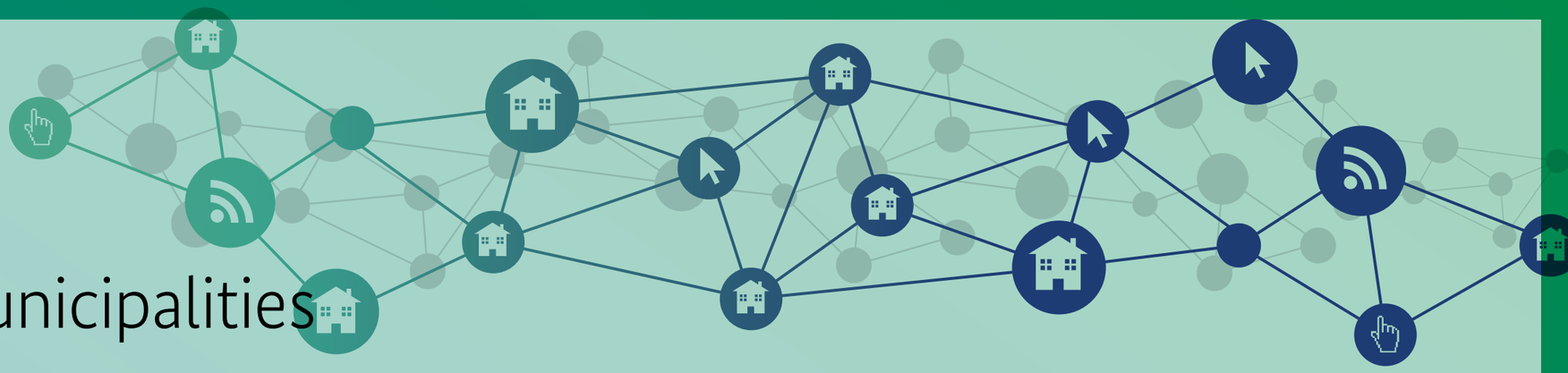
RESPONDING TO CRISES

In particularly serious cases, the IT Situation Centre grows into the National IT Crisis Response Centre. Specialists from various fields work closely together in this centre to quickly restore normality in a crisis situation.

In an emergency, the new infrastructure allows up to 100 IT security specialists to work together in an orchestrated manner. Around 19,000 metres of network cable were laid to connect the rooms and systems required to operate the situation centre. This corresponds to the length of a motorcade across all BSI properties in the federal city of Bonn.

CONCLUSION AND NEXT STEPS

With the new National IT Situation Centre, the infrastructure is in place to substantially increase cybersecurity in Germany. With the BSI as a central office in the federal-state relationship, the national situation picture could be further standardised and specified. The federal states and local authorities would also benefit from an ad hoc threat picture and centralised sensors to better anticipate threats. To this end, the threads can come together in the new situation centre to protect Germany against threats from cyberspace across the country. ■



Cybersecurity in Rural Districts, Cities and Municipalities Expanding Together

The BSI Brings Together the Federal Government, Federal States and the Municipal Sector to Jointly Develop Strategies for Increasing the Level of Cybersecurity in Municipalities.

By Stefanie Euler, Head of Division IT Security Consulting for State and Local Governments

Municipalities are increasingly being targeted by cyber criminals, as numerous recent attacks have shown both frighteningly and impressively. Such attacks regularly have far-reaching consequences for local authorities – and therefore for citizens. The BSI is therefore promoting cooperation between the federal government, federal states, local authorities, associations and service providers. After all, cybersecurity is a joint task that everyone must tackle together.

The cybersecurity situation in Germany is worrying. The damage to the economy, administration and society caused by cyberattacks runs into billions of euros. Attacks using so-called ransomware in particular are currently widespread, as they represent a lucrative business model for cyber criminals. In addition, there is growing professionalisation on the perpetrator side and an increasing number of security vulnerabilities. Attacks can affect anyone. For example, the BSI has observed a shift in cyber attacks using ransomware: It is no longer just large, solvent companies that are now being targeted, but increasingly also small and medium-sized organisations as well as state institutions and local authorities.

AN AVERAGE OF TWO ATTACKS PER MONTH LOCAL AUTHORITIES

On average, more than two successful ransomware attacks on local authorities or municipal companies are reported every month.

The example of a municipal IT service provider that fell victim to a cyberattack last year shows the vulnerability: it discovered encrypted data on servers and reported the attack. As a precautionary measure, the majority of IT systems were shut down – with the result that more than one hundred municipal administrations were unavailable or only partially accessible. The websites of the administrations were also affected. If a central IT service provider goes down, this has an impact on many local authorities and therefore also on the general population.

LOCAL AUTHORITIES THEREFORE NEED SPECIAL PROTECTION

The task of arming themselves against cyber attacks must therefore be at the top of the agenda for local authority decision makers. However, the federal and state governments must also support local authorities – after all, protecting the administration is a joint task for all stakeholders that can only be achieved together.

However, individual consultations for local authorities are not feasible due to their large number. The BSI therefore works closely with numerous committed multipliers at local authority level. Local authorities can access handouts and recommendations on specific topics, as well as specific support documents and working aids – whereby all support services are practical and scalable. They help those responsible to get started with information security and to protect their systems and networks effectively.

Another tool for implementing information security as efficiently as possible in local authorities are so-called IT-Grundschutz profiles. Using these templates for information security, companies and authorities can create profiles for use cases and then make them available to other interested parties. Users who have similar security requirements can use this template to check the security level of their institution in a resource-saving manner. The BSI supports representatives from the federal states and local authorities in the development and provision of these IT-Grundschutz profiles, among other things.

The BSI also organises various events for the target group of local authorities. For example, the BSI has designed the "Local Authorities Roadshow" format and organised it together with a number of federal states. This is a virtual series of events designed to raise the level of cybersecurity security in the municipal environment.

Cooperation agreements between the federal states and the BSI also address support for the municipal level. In order to jointly raise cyber and information security to a higher level, the BSI has so far concluded cooperation agreements with six federal states. The contractual partners support each other as part of the cooperation agreements in order to increase information security efficiently and effectively. The cooperation requirements include, for example Exchange of cybersecurity information, warnings, work shadowing, support with incident reports, presentations to raise awareness of the topic of cyber security, or joint information events for citizens.

WHAT LOCAL AUTHORITIES NEED

The basis for the various programmes is the practical needs of local authorities and how they can be met. For example, a "BSI in dialogue" event held in Berlin in February 2024 focused on cybersecurity in local authorities under the key question "How can we fundamentally contribute to strengthening local authorities in the area of cyber and information security?". The BSI invited representatives from the federal government, federal states and local authorities as well as service providers and associations to discuss and jointly develop lines of action, some of which included concrete measures – always with the aim of quickly and effectively increasing cyber security in local authorities.

Several specific lines of action were identified, which are now being pursued either by the BSI or individual participants. The focus was on the following topics: improving networking, possibilities for IT bundling, creating a legal framework in the federal states, providing sufficient resources, possible centralised services, conducting cybersecurity exercises, establishing standards and the trending topics of AI and the cloud.

From the BSI's perspective, the conclusion of this dialogue is that The current offerings, including the BSI's information security advice for federal states and local authorities, are target-oriented and should be pursued and expanded where possible. This also includes the checklists from the "Weg in die Basis-Absicherung" (WiBA) project, which make it easier for local authorities to get started with IT baseline protection and enable them to implement effective security measures in a resource-efficient manner. The previous exchange formats are also to be continued in the interests of networking and knowledge sharing. In particular, the "BSI in dialogue" format between the federal government, federal states and local authorities is to be continued, the "Local government roadshows" are to be made permanent and additional similar dialogue and information formats are to be designed by the BSI, the federal states and municipal umbrella organisations.

EXPAND COOPERATION BETWEEN THE FEDERAL AND STATE GOVERNMENTS

The dialogue between the federal government, federal states and local authorities shows that we are on the right track: We are on the right track, but there is still a lot to do to counter the increasing number of attacks and thus ensure reliable and comprehensible administrative action in cities, districts and municipalities.

In addition to organisational and technical measures, the legal possibilities must also be further expanded. The legal frameworks of the federal and state governments are already being fully utilised. In order to take account of the increasing threat situation, further (constitutional) legal options should be created so that the federal, state and local authorities can act quickly, efficiently and therefore effectively. This requires, among other things, the possibility of supporting each other in specific incidents, sharing work and creating a joint picture of the situation. Because one thing is clear: only together will we be able to counter organised crime and targeted attacks in order to ensure successful digitalisation and, ultimately, municipal services of general interest. ■

Information security from users for users: Provision of IT-Grundschutz prof les:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifz ierung/IT-Grundschutz/IT-Grundschutz-Prof le/it-grundschutz-prof le_node.html

Five Years of Cybersecurity in Freital

Great Team Spirit and Meaningful Tasks at the BSI's Second Office

By Julia Wiebe, Division Cyber Air Security

In July 2019, the official go-ahead was given for the opening of the second BSI site in Freital, Saxony. Today – five years later – more than 170 colleagues are already working at the site between the Elbe Valley and the Eastern Ore Mountains. Osterzgebirge mountains are helping to build Cybernation Germany.

Prof. Thomas Popp, State Secretary for Digital Administration and Modernisation of Administration and CIO of the Free State of Saxony

The BSI site in Freital has been strengthening cybersecurity in the Free State of Saxony since 2019.

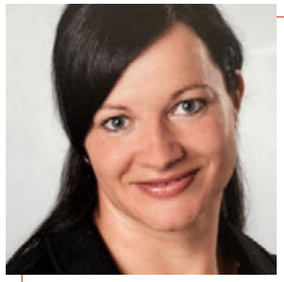
As a federal state that is home to the Silicon Saxony high-tech cluster in the Dresden area, the BSI site, with its focus on next-generation mobile technologies, fits perfectly into the existing structure of teaching, research and business – including the Institute of Communications Engineering at TU Dresden, the Barkhausen Institute and research facilities such as Vodafone's Tech Innovation Centre. Security is also a basic prerequisite for the successful digitalisation of administration. In order to be prepared for threats from cyberspace and to be able to get back to work quickly in an emergency, we need to intensify cooperation at all levels. We are doing this in Saxony as a state administration with the local authorities through a joint integrated IT security architecture. However, intensive cooperation is also necessary with the federal government.

I am therefore delighted that we signed a cooperation agreement with the BSI in November last year. We work together on cyber defence, support each other in the event of IT security incidents and work together to further educate citizens on the topic of cyber and information security. At last year's Saxon roadshow on cybersecurity under the motto ‚Digital? But secure!', which was attended by over 3,000 people in 13 Saxon cities, we were able to gain the BSI as a partner, which enriched the programme with its content.

I would also like to emphasise the close cooperation in protecting the European Capital of Culture Chemnitz 2025. Next year, the whole of Europe will be looking towards Chemnitz and the cultural region. It will be a special celebration. I am looking forward to continuing our cooperation with the Federal Office for Information Security.

The focus of the work that is being done in Freital includes the development of secure 5G/6G, digital consumer protection and the cybersecurity of civil aviation. Three technical experts provide examples of the broad range of tasks at the Freital site.

- **30th april 2024:** Official handover of keys for renovated property
- **15th december 2023:** Establishment of the "Cyber Aviation Security" Divison
- **30th august 2023:** Opening of 5G/6G Security LAB (TEMIS)
- **01st december2022:** Start of in-house operation of the BSI Service Centre
- **01st january2022:** 100 employees at the Freital site
- **december 2021:** Introduction of the IT security label
- **16th june 2021:** First publication of the report on digital consumer protection
- **1st july 2019:** Signing of the declaration of intent



"There is a great team spirit"

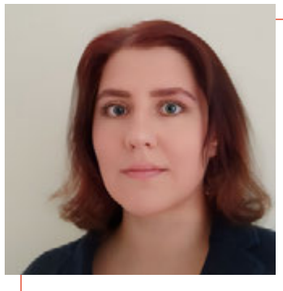
When I was looking for new professional challenges a year ago, I discovered the BSI's job advert for a position in the office of the Cybersecurity for Business and Society Divison. There are many reasons why I enjoy coming to work: Our Divison deals with social and economic aspects of cybersecurity security, which is interesting and never boring. For me personally, the opportunities for further training and the family-friendly environment are absolute plus points. After my first year at #TeamBSI, I'm glad I took the plunge and moved to Freital. At BSI, we not only have numerous specialist topics, but also many opportunities to get involved, for example when it comes to the culture of cooperation and cohesion among colleagues. For example, at regular team-building events such as the summer party or Divisonal events.

Kristin Lindner, Cybersecurity for Business and Society Divison

"Society benefits from our work"

Even during my Master's degree in Public Administration, I was enthusiastic about the topics of administrative digitalisation and eGovernment. The opening of the BSI site in Freital gave me the perfect opportunity to focus more on projects at the interface between technology and administration. As a consultant here, I am responsible for the BSI's voluntary IT security label. Together with my colleagues, I am working on making the cybersecurity security of consumer products more transparent and incentivising manufacturers to design their digital products securely. Our contribution to security in the digital world, the social benefits of our work and my great team motivate me every day for my job in #TeamBSI.

Paul Trinks, IT security labelling Divison



"We have good career opportunities"

I took the plunge into the public sector three years ago and have never regretted it. I started at the BSI as a consultant in information security consulting. In this position, I was able to take on responsibility right from the start and, among other things, introduce digital tools in my specialist area. I am particularly enthusiastic about the open culture and the strong team spirit at the BSI. We all pursue the same goal: to add value to society. BSI also promotes the personal and professional development of its employees. In addition to an extensive training programme, internal promotion opportunities are offered. I took advantage of this and took over the management of a newly established divison in March 2024. Together with my team, I am actively helping to ensure that cybersecurity security in civil aviation is strengthened in the long term and that flying remains safe.

Sandra Teichert, Cyber Aviation Security Divison Principle

BSI
20. Deutscher
IT-Sicherheitskongress

Focus on Cybersecurity:
The German IT Security Congress Turns 20

For the 20th time, the BSI has organised this high profile specialist event at which representatives from admi nistration, business, science and society discuss current topics and issues relating to cybersecurity. To mark this anniversary, the BSI Magazine editorial team spoke to former BSI President Michael Hange. He was a member of the BSI's founding staff and attended all IT security conferences from day one until his retirement in 2015. Even in retirement, he still attends some of the presentations at the online congress.

Mr Hange, how did the first IT Security Congress come about? What was the aim, who was the driving force behind it at the BSI, which still had a relatively small number of employees at the time?

Michael Hange: The first German IT Security Congress took place in 1990 in the run-up to the founding of the BSI and against the backdrop of German reunification, which was a very exciting time for me on the BSI's founding staff. Representatives of the central cipher organisation of the GDR also took part in the congress. The BSI was only launched in 1991 with working areas from different security authorities. The joint aim of the Federal Ministry of the Interior and the founding president Otto Leiberich was to use the congress in 1990 to present the future BSI and its topics, which until then had only been known to insiders, to a wider specialist audience for the first time. With the participation of external speakers, the BSI presented itself as a new technical authority that was not only focussed on the administration, but also explicitly included the economy and citizens. Due to the parliamentary legislative process for the establishment of the BSI, the authority was to become better known to the public as a trustworthy partner.

Are the issues of that time still the issues of today?

Hange: At every IT security congress, the aim was certainly to address current specialist topics "at the cutting edge". The change in topics was always determined by the rapid technological development and the intensifying threat situation from the goldfish pond of the nineties to today's shark tank. In addition to cryptography, the first IT Security Congress focussed in particular on certification according to international standards for the manufacturers of IT products. Due to the associated interference in competition, a legal basis for certification had to be created in the BSI Act. The presentation of the first IT-Grundschutz manual at the 1992 congress is certainly one of the thematic milestones in the further development of the event. With the IT-Grundschutz manual, a standard for IT security management was set in the economy as well as in the federal administration. In 2000, the Loveletter virus ensured that the topic of Internet security for use in the private sector was included more prominently in the congress programme. The congress was also a forum for discussions, e. g. in the run-up to the introduction of legal initiatives on IT security – as in the case of sovereign documents. Over the years, different target groups were addressed and sensitised in an increasingly differentiated manner alongside the technical specialist community. In addition, cooperation between the relevant stakeholders has been sustainably promoted.

A quote from the 2003 conference proceedings reads "pooling distributed forces for a common goal" – the motto of the current IT Security Congress is "Cooperation wins": Why are co-operation and networking still so important for information security today?

Hange: Cooperation and information exchange are essential in cybersecurity. To this day, the IT Security Congress is designed as a platform for an exchange on a wide range of IT security topics – with the aim of being at the cutting edge of knowledge at every edition. The BSI contributes its technical expertise and at the same time attaches great importance to the participation of experts from science, industry and administration, so that they can present their latest solutions. Today's online format has the advantage that several thousand interested parties can now follow the presentations free of charge.

"To this day, the IT Security Congress is designed as a platform for an exchange on a wide range of IT security topics – with the aim of being up to date with the latest findings at every edition."

What role does the advisory board play for the congress?

Hange: With experts from science, business and administration, the advisory board stands for the independence of the congress content; individual members of the advisory board have been contributing their expertise to the programme for decades. The congress advisory board defines the programme together with BSI managers, evaluates and selects the presentations submitted. Even at the first congress, it became clear that the event is not centred on BSI-centric opinions, but is shaped by the expertise of the specialist community.

Can you tell us a highlight from the first few years?

Hange: I still remember my first presentation, which I gave at the IT Security Congress in 1991. It was a presentation on cryptology to an audience, some of whom had no specialised knowledge of the subject. During the preparations, I naturally realised that it was less important to convey cryptology in depth than to give a talk with understandable messages about cryptographic concepts and their applicability – even for normal IT users. It was a real challenge to avoid the usual "cryptic" jargon with lots of technical terms. This is certainly still a challenge for every lecturer today and you learn it in practice.

What is the secret to the success of the German IT Security Congress?

Hange: Firstly, the good technical preparation of the presentation topics and slots. The selection of topics is like a magnifying glass on the current and pressing issues and problems in IT and cybersecurity. On the other hand, the qualified organisation of the congress was particularly appreciated by the exhibitors. Networking is also a decisive factor at the congress. While the participants used to meet in person at the Stadthalle Bad Godesberg, the congress is now the largest digital class reunion on cybersecurity in Germany.

What do you wish for the German IT Security Congress?

Hange: I hope that the BSI will continue to address the relevant topics for a wide range of target groups in the coming editions of the congress and continue to pursue its successful co-operative approach.

You have been retired for some time now: do you follow the congress online?

Hange: The congress has certainly changed with the live format, but I still find it very exciting. I've been out of the day-to-day business for a few years now. However, as an IT user, I follow individual presentations at the online congress with interest. ■

BSI Market Surveillance – For more IT Security in the Consumer Market

A Look behind the Scenes: How BSI market Surveillance Works with the Manufacturers of Labelled Products

By Inke Gelfert and Daisy Kunze, Division Market Market Surveillance of certified Service Providers and Products

What to do if security vulnerabilities in a product become known? How does an ad hoc technical conformity check work? BSI Market Surveillance provides insights into the processes surrounding the new IT Security Label, which manufacturers and service providers use to label their IT products. In doing so, they attest that certain security features are present.

Before applying for the IT Security Label, manufacturers must test their products for conformity with the BSI's security requirements. To do this, they must provide essential technical information about the product and describe in detail which methods and procedures they have used for the conformity test. On this basis, the BSI assesses whether the information is sufficiently documented and if vulnerabilities are currently known. However, as the security features of IT products can change over time, the BSI does not test the products on a predetermined date, but monitors them during the validity of the label through BSI Market Surveillance. The efficient application process in combination with downstream Market Surveillance promotes trust in the IT Security Label and does justice to the fast-moving product cycles on the consumer market.

After the official handover of the IT Security Label to the applicant, the work of the BSI Market Surveillance begins. During the validity of the label, it checks whether the labelled products comply with the conformity specifications assured in the manufacturer's declaration. This is done both proactively and reactively.

AN IT SECURITY LABEL HAS BEEN APPROVED FOR USE – AND NOW WHAT?

For the duration of the granting, the manufacturer agrees to inform the BSI about possible vulnerabilities in its products, to provide security updates and to comply with the applicable security requirements. The BSI Market Surveillance monitors these security features for the duration of the approval. It checks the products for compliance, responds to vulnerability reports and maintains the security information of the products on the BSI website. Market Surveillance can consult application documents, technical documentation and manufacturer documents or carry out test purchases in order to technically check the products.

HOW DOES PROACTIVE MARKET SURVEILLANCE WORK?

Market Surveillance samples proactively and without cause. An initial preliminary technical inspection is carried out either by the BSI or by recognised IT security evaluation fascilities.

The main points of a proactive inspection are

- Checking the conformity of the product with the underlying IT security requirements, such as the standards for secure broadband routers, for secure e-mail transport and the ETSI standard for Consumer Internet of Things (IoT)
- Verification of compliance with manufacturer obligations in the event of security vulnerabilities, following reports to the BSI

In addition, labelled products can be subjected to in-depth testing. The test objects are analysed specifically with regard to the required IT security standards. This can also include penetration tests or interface tests, for example, in order to uncover possible non-conformities. The findings from the in-depth inspection are subsequently discussed with the manufacturer of the product bearing the IT Security Label.

WHAT CAN TRIGGER REACTIVE MARKET SURVEILLANCE?

Weaknesses in the product or in the technologies used can give rise to an investigation. Sometimes manufacturers gain their own insights and come forward or there are indications from third parties. Various security information come together in the BSI's IT Situation Centre. If the sources of information provide security-relevant hits on labelled products, the Market Surveillance checks the potential threat risk in collaboration with other BSI colleagues.

WHAT HAPPENS AFTER A VULNERABILITY IS FOUND?

If a vulnerability is found, Market Surveillance contacts the relevant manufacturers and service providers. This often results in a close dialogue, which leads to the swift provision of the necessary update. Experience to date has shown that the manufacturers are very keen to maintain the security of their products.

FOR EXAMPLE, WHAT PREVIOUS OCCASIONS HAVE TRIGGERED SUCH A REACTIVE ACTION?

One reason for contacting email service providers, for example, was the "Simple Mail Transfer Protocol (SMTP) Smuggling" vulnerability. With this vulnerability, attackers take advantage of the fact that different SMTP implementations interpret the marking of the end of an email message differently. This allows forged emails to be sent (spoofing) and even authentication mechanisms to be bypassed. Warnings, such as a spam mark in the subject line, are also no longer valid.

The Terrapin security vulnerability was another reason for market surveillance action. This can weaken encrypted Secure Shell (SSH) connections on routers, allowing an attacker to delete data from a secure SSH connection via a man-in-the-middle attack in order to reduce the security of the connection.

The BSI Market Surveillance worked with the manufacturers to check whether the labelled products were actually affected. If this was the case, the vulnerability was quickly rectified by the manufacturer.

HOW ARE CONSUMERS INFORMED?

Once the updates have been made available, the BSI updates the relevant product information page for consumers. The quickest way to get there is to scan the QR code on the IT Security Label. The product information page contains consumer-friendly information about the security features of the product or known vulnerabilities. ■

Further information:

www.bsi.bund.de/it-sik/hersteller

For a Healthy #TeamBSI

At BSI, We Focus on Prevention – Both in Terms of Cybersecurity and the Health of Our Employees.

By Kirsten Kampmann and Miriam List, Division Human Resources Development

At BSI, we focus on the physical and mental health of our employees. Our comprehensive health management programme goes far beyond the physical break – we take a holistic approach and interlink measures on many levels. Our aim is to promote both the health and the satisfaction and motivation of our employees.

The diverse demands and fast pace of today‘s working world and private life also pose a challenge to health. That‘s why we at BSI are focussing on holistic health management with the motto Healthy #TeamBSI, which is more than just taking part in the company run. Health is our top priority, because we can only advance cybersecurity in Germany with healthy employees. At BSI, mental and physical health are taken into account at all levels and in all processes – for example in personnel development, which interlinks strategies and measures in the areas of health management, leadership, lifelong learning and internal collaboration. After all, motivated employees who feel valued by their employer BSI perform well and increase the potential for innovation.

INVOLVEMENT OF ALL EMPLOYEES: THE KEY TO CUSTOMISED SOLUTIONS

At BSI, we encourage employee participation and two-way communication. As with our task of sensitising the state, economy and society to cyber-security and at the same time strengthening it, we rely on the principle of prevention, detection and response in health management. We therefore regularly survey all employees on topics that have a particular impact on health in the work context. These include leadership, social relationships, a sense of belonging and meaningful work tasks. We systematically record the employees‘ assessments and can thus visualise potential for improvement. Improvement measures are implemented – sometimes on a Divison-specific basis. However, it is not only these areas of action that serve as an important foundation. The surveys also reveal strengths and resources at BSI, which we utilise to create a healthy working environment. This form of employee involvement enables us to continuously improve working conditions and thus contribute to a healthy #TeamBSI.

“At BSI, we attach great importance to a culture of appreciation and participation. Because only in an environment based on mutual respect and understanding can we promote the long-term well-being and performance of our team. Health is more than just the absence of illness – it is a holistic state on a mental, physical and social level. In occupational health management, we support this by creating healthy framework conditions and encouraging people to consciously engage with their own health.”

Kirsten Kampmann, Health Management

“Strengthening resilience is not only important in the IT world, but also with regard to the health of our employees.”

Claudia Plattner, President of the BSI

In a short survey, the pulse survey, for example, we asked employees to assess their own mental health in digital collaboration. The pleasing result: 85 per cent of employees rated the work-life balance in particular as positive. Fortunately, the assumption that the digital way of working would lead to a feeling of social isolation did not materialise – team cohesion and social interactions are not limited to face-to-face encounters. At the same time, however, it also became clear that the hybrid working world is associated with new challenges. We are responding to this with various approaches to collaboration.

For us, the active involvement of managers is a matter of course and indispensable. They are a major lever and have a great deal of influence due to the breadth of their impact – especially at the top management level. For example, all Divison heads meet twice a year to discuss health-related activities and processes and decide on specific measures.

DIVERSE MEASURES TO PROMOTE HEALTH

In addition to the structural approaches to health management, a healthy working environment is important to us. We are also concerned with strengthening individual health awareness and supporting healthy working habits and behaviour.

Due to our predominantly sedentary work, it is important to integrate exercise into our daily routine. We have various programmes for this:

- **Digital moving break**
- **Electrically height-adjustable desks**
- **Annual participation in the company runs in Bonn, Dresden and Saarbrücken**
- **Annual steps challenge**
- **Cooperation with a health provider**

In addition to the sporting activities, we organise informative keynote speeches on various health topics. In addition to the idea of prevention, we also aim to impart knowledge and expand expertise in the following areas

- **Mental health (e.g. dealing with stress)**
- **Healthy nutrition**
- **Reconciling work and family life**

Prevention also includes free flu vaccinations at our locations. This protects the health of our employees and prevents absences due to illness. In addition to all structural and cross-organisational measures, the individual needs and challenges of each employee must not be neglected. Our social counsellor from the Federal Ministry of the Interior offers all employees a sympathetic ear and can provide expert advice on personal matters or in difficult life situations. The company integration management programme also offers individual support after a long period of illness.

"The social counselling and occupational integration management services address the individual needs of employees. The specific situation of the person concerned is addressed and solutions are developed together.

These individual discussions also provide us with valuable insights for the entire organisation. This allows us to bundle them and dovetail them with other areas, such as occupational health and safety or management development."

Miriam List, Health Management

"We all often only appreciate good health when it is impaired. Health is a valuable asset that we should protect! Not only is it better to live a healthy life, but health also has a positive effect on our performance!"

Sandro Amendola, Director of Section SZ

A HEALTHY #TEAMBSI IS ALSO AN EFFICIENT AND INNOVATIVE #TEAM BSI

We see health management as an investment in the development of our employees and therefore in the long-term success of BSI. Involving employees in a targeted manner, implementing a wide range of health measures and actively promoting healthy collaboration are the ultimate goals of personnel development. In this way, we create a working environment in which everyone feels comfortable and can realise their full potential. Healthy and motivated employees are not only more productive and innovative, but also more efficient and satisfied. BSI keeps its finger on the pulse in order to understand the needs of #TeamsBSI and continuously optimise working conditions. Together, we are shaping a healthy and successful future – because health is not just a promise, it is our lived reality.

Healthy #TeamBSI: Strong together for a healthy future! ■

Further information:

https://www.bsi.bund.de/DE/Karriere/Arbeiten-im-BSI/Einblicke/Ein-Tag-im-BSI/Tagesablaeufe/Kirsten_Kampmann/Kirsten_Kampmann_node.html

30 Years of IT-Grundschutz: 30 Years of Information Security

A Brief Look Back, a Big Look Forward to the Future

By Petra Alef and Holger Schildt, Division BSI Standard and IT Grundschutz

30 years ago, the BSI published its first IT security recommendations under the name "IT Grundschutz" – a milestone in the history of information security. IT Grundschutz remains dynamic in line with its own guiding principle: information security is not a status, but a process. We take a brief look at the past before looking to the future.

About IT-Grundschutz

The IT Grundschutz programme of the German Federal Office for Information Security (BSI) is a tried and tested method for increasing the level of information security in public authorities and companies of all sizes. The offerings of IT Grund schutz are considered the benchmark in administration and business when it comes to securing information and setting up an information security management system (ISMS). A systematic approach makes it possible to identify and implement the necessary security measures. The BSI Standards provide proven procedures for this. The IT Grundschutz Compendium formulates specific requirements with the IT Grund schutz modules.

Three decades is already a long time in the analogue world – in the digital world it is an eternity. Accordingly, IT-Grundschutz Three decades is already a long time in the analogue world – in the digital world it is an eternity. Accordingly, IT-Grundschutz has seen many changes since the first edition of the IT-Grundschutz manual was published in 1994. IT-Grundschutz has always been dynamic, whether in its early days when the Internet became a mass phenomenon or today, when it comes to the ongoing development of digitalisation in public authorities and companies, when sub-areas such as artificial intelligence (AI) are developing rapidly and, above all, when the vision of a cyber nation Germany is to become reality. IT baseline protection has established itself as a nationally and internationally recognised standard in the area of information security.

From the very beginning, the basic idea was to make IT security recommendations as practical and flexible as possible. Users were given a modular concept to help them help themselves. It started with a FAQ list and 15 pilot IT-Grundschutz modules. These modules each describe typical threats for a specific aspect of information security (e. g. the use of servers) and, in the early days of IT-Grundschutz, security measures and, from the IT-Grundschutz-Compendium onwards, requirements. Over the years, this has become a comprehensive and up-to-date compilation of methods, recommendations and standards. Local authorities as well as state and federal authorities work with it, as do local craft businesses, SMEs and DAX-listed companies.

In addition, it has been made possible to prove information security to customers, service providers and employees with the help of certificates and test certificates. An ISO 27001 certificate in accordance with IT-Grundschutz still demonstrates the importance of information security in an organisation today.

Practical relevance and flexibility are still fundamental elements of IT-Grundschutz protection today and will remain so in the future. The pace of development in information security alone requires that IT-Grundschutz is continuously updated. The following overview presents the most important current projects and plans.

PUBLICATION OF THE BCM PRACTITIONER TRAINING CONCEPT

Whether a data centre fails, a production facility is destroyed as a result of a natural disaster or there is a cyberattack on the entire IT infrastructure – public authorities and companies are exposed to a constantly growing number of potential threats that can lead to an interruption of business operations that could threaten their existence.

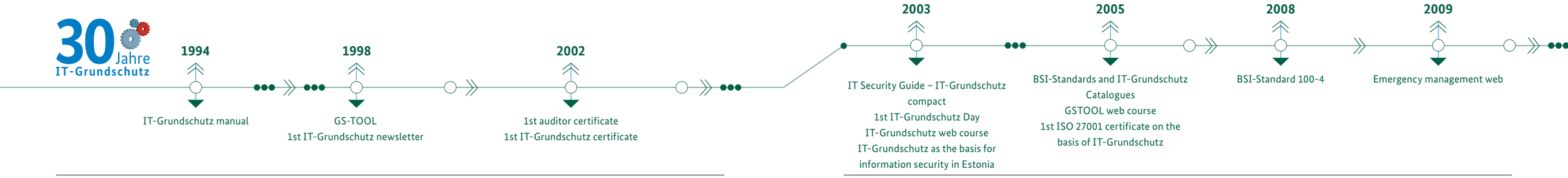
How can you protect yourself? Among other things, business continuity management (BCM) is becoming increasingly important. Alongside information security and crisis management, BCM is the tool for organisational resilience. However, many users still find it difficult to plan and structure a suitable business continuity management system (BCMS). There is a high demand for qualified personnel who can competently support implementation with recommendations and concrete measures.

The BSI has the answer to this need: the modernised BSI-Standard 200-4 BCM was presented in 2023. Based on this, the BSI has developed a new training concept for BCM practitioners. Since the beginning of 2024, the training course has been available from cooperating training providers.

The BCM practitioner training is a supplement to the IT-Grundschutz practitioner and consultant and is aimed at business continuity officers (BC officers) and those interested in BC. It provides basic knowledge of the entire BCMS process in accordance with BSI-Standard 200-4 and is supplemented by practical examples and explanations.

Further information

https://www.bsi.bund.de/dok/BCM-Praktiker



30 Jahre IT-Grundschutz

"Whatever happens in the field of digitalisation and information technology, IT-Grundschutz will remain dynamic and respond to it."

Holger Schildt, Head of Division of SZ 13 since 2017

Facts about IT-Grundschutz

- The first IT Grundschutz consisted of a FAQ list.
- The results of a fundamental modernisation of IT Grundschutz were presented in 2017. The content was focussed and streamlined, and new topics, procedures and IT trends were included.
- The current version of IT Grundschutz contains four BSI Standards and 111 IT Grundschutz modules in the IT Grundschutz Compendium.
- 35,985 subscribers receive the IT Grundschutz newsletter and 14,680 subscribers receive information about the latest news via the BCM newsletter.
- There are currently 19 IT Grundschutz profiles on different application scenarios available on the BSI website.
- The BSI has developed training concepts for the IT Grund schutz practitioner, the IT Grundschutz consultant and the BCM practitioner.

REDUCTION OF DOCUMENTATION EFFORT

In 2023, a project was carried out on the documentation effort involved in establishing an information security management system (ISMS) in IT-Grundschutz. The aim is to reduce the documentation effort to the necessary minimum in future. To this end, the current requirements were reviewed with regard to their necessity. At the same time, the previous requirements for documentation were harmonised in order to provide more clarity for implementation in the future while retaining freedom in the actual design.

The first tools developed from the project will be made available to users as early as 2024. This will enable an initial reduction in the amount of documentation required for IT-Grundschutz in the near future.

THE TENSION BETWEEN CONTINUITY AND ADAPTABILITY: AN OUTLOOK

IT-Grundschutz is constantly being developed further, both to keep pace with technical developments and to meet the needs of users. After all, one of the BSI's goals is to increase the resilience of companies and authorities and to organise information security in a pragmatic way. IT-Grundschutz operates in an interesting area of tension. On the one hand, continuity in the design of holistic, procedural information security is essential. On the other hand, the rapid development in the digital sector also requires IT-Grundschutz to be highly adaptable. In addition, many users would like to see further simplifications – a challenging wish to realise for a complex topic. Anyone striving for holistic information security, for example by setting up a comprehensive ISMS, has a time-consuming and resource-intensive process to master.

These are all challenges that IT-Grundschutz will continue to face in the future. IT-Grundschutz is being further developed in an agile manner with the aim of reducing the scope and the documentation effort involved in implementation to the necessary minimum, prioritising the requirements and enabling the use of automation tools as far as possible. The first version of the further developed IT-Grundschutz will consist of the introduction of a successor to the IT-Grund-schutz-Compendium. Parallel to this revision, the 2023 edition of the IT-Grundschutz-Compendium will be updated as re-quired and necessary and new modules will be added where necessary. Piloting of the further developed IT-Grundschutz-Compendium is planned for the end of 2024/beginning of 2025. During a transitional period lasting several years, the current IT-Grundschutz and versions of the enhanced IT-Grundschutz will continue to exist and be applicable side by side. The successful implementation of IT-Grundschutz is also to become measurable, and stronger synergies with other BSI requirements are also planned.

At the same time, lessons learnt from past projects will be incorporated into further development. Experience from the project group "Paths to basic protection" shows, for example, that there is a pleasing interest in information security on the one hand, but on the other hand there is also a need to further increase the practical orientation of IT-Grundschutz. ■

Would you like to be informed about the latest news from IT-Grundschutz? Then subscribe to our IT-Grundschutz newsletter:

https://www.bsi.bund.de/newsletter

2012 – Implementation framework (UMRA) for BSI-Standard 100-4

2016 – IT-Grundschutz Catalogues comprise 100 modules

2017 – BSI-Standards 200-1, 200-2 and 200-3 IT-Grundschutz-Compendium 1st IT-Grundschutz profile

2018 – Online course on modernised IT baseline protection 1st ISO 27001 certificate based on IT-Grundschutz according to the IT-Grundschutz-Compendium

2019 – Certificate after the basic protection IT-Grundschutz practitioner and consultant

2023 – BSI-Standard 200-4

2024 – BCM practitioner

Remote Work Will Remain Secure in the Future

Modern Platform Solutions Enable a Vibrant App Ecosystem for Classified Information.

By Lars Bruchhaus, Jan Metzke and Yvonne Omlor, Division Classified Information Systems and Approved Products (CIS)

Who would want to do without it? Remote working has revolutionised the world of work in many sectors – employees often decide for themselves how, when and where they work. Mobile applications make it possible. However, confidentiality, availability and integrity must also be guaranteed for remote working. In the future, platform solutions and app ecosystems will allow even more flexibility and significantly expand the range of functions.

Mobile communication is one of the most innovative and rapidly developing areas of the IT industry. The "new normal" means that work is expected to be done anywhere and at any time. This is possible with mobile devices, which have become universal tools thanks to easy-to-install apps and their performance.

However, this development also harbours risks: If mobile devices are lost or even stolen, potentially confidential data is at risk. Misuse and manipulation of the devices also pose risks, such as the unnoticed monitoring of users.

"(ENSURING) MOBILE SECURITY IN FEDERAL ADMINISTRATIONIN THE FEDERAL ADMINISTRATION

The BSI has been working with various manufacturers for many years on solutionsfor secure mobile working within the federal administration, including handling classified information up to the classification level VS – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD).. With these solutions, the classic security triad is implemented: "Data at Rest" – secure storage on endpoint devices, "Data in Use" – security when working with the data and "Data in Transit" – secure connection to the backend. Mobile devices are managed and securely configured using Mobile Device Management.

Although mobile operating systems often have good security mechanisms, these are difficult to evaluate without close cooperation with the manufacturers due to the complexity of the systems and the high development dynamics. As a result, manufacturers of secure mobile solutions have often been forced to develop their own security mechanisms for products such as SecurePIM Government SDS or SecuSUITE for Samsung Knox. In this way, a high, verifiable level of security can be achieved, but functional extensions often prove to be complex and difficult to implement.

For this reason, the BSI has expanded its cooperation with the manufacturers Apple and Samsung in recent years and evaluated native security functions in the iOS/iPadOS and Samsung Knox platforms. This verified platform security is the basis for the solutions "indigo" and, in future, "Knox Platform for Enterprise Knox Native Solution" (Knox Native).

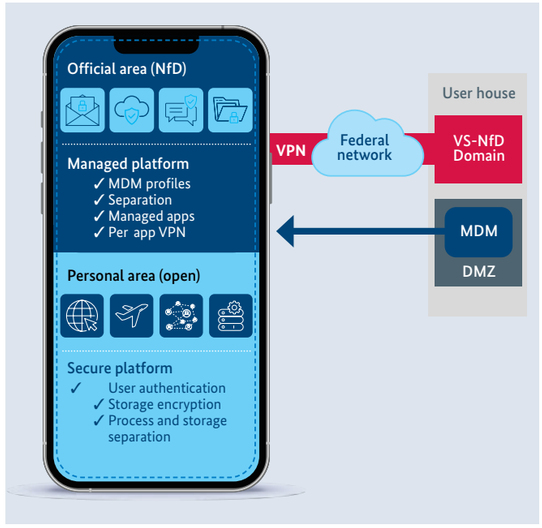


Figure 1: Secure mobile platform: target architecture

PLATFORM SOLUTIONS: INDIGO AND KNOX NATIVE

Native security functions form the foundation for the indigo and Knox Native solutions. Both already enable secure access to emails, calendars and contacts at VS-NfD level via the pre-installed native apps. In addition, indigo offers VS-NfD-compliant S/MIME encryption and Knox Native provides access to notes. The underlying encryption in indigo is based on Apple's natively installed security anchor, the Secure Enclave, while Knox Native relies on a Java Card applet developed jointly with the BSI that runs in the certified embedded Secure Element from Samsung. The separation between personal and business apps is made possible by the operating system's separation mechanisms and an evaluated, native VPN technology (Fig. 1).

The native security functions not only protect the internal network and improve battery life. They also create an experience that users are familiar with from their private devices. Thanks to their scalability, native security functions also form the basis of a living ecosystem that gradually and continuously expands the functional scope of mobile solutions through the dynamic inclusion of additional secure apps.

OUTLOOK FOR THE FUTURE: BUILDING AN APP ECOSYSTEM

With TrustOwl & SecuFOX as intranet browsers and SecuOFFICE & TrustDok for document processing, the first apps based on the native security mechanisms of the indigo platform are now available. The Wire and SecuVOICE apps for secure communication are also available to users of the released indigo solution. It is also possible to continue using previous solutions such as SecurePIM in parallel as part of a smooth migration.

By utilising tested security functions, it will also be possible in future to provide other apps and in-house developments that are already available for the federal administration. To this end, the BSI is developing an easily accessible process with a testing laboratory (Fig. 2). Both the existing apps and the in-house developments will be subject to a review. The correct use of the security functions that have already been evaluated is verified. In addition, valid processes for troubleshooting and the lifecycle are ensured. After successful testing, the apps can be used in the platform solutions.

The modular structure of the ecosystem allows for continuous further development. Future apps can be easily integrated without the need for extensive new developments for the platform. This means that the federal administration can continue to benefit from innovative, customised solutions for secure, mobile work in the future while ensuring a high level of data protection. ■

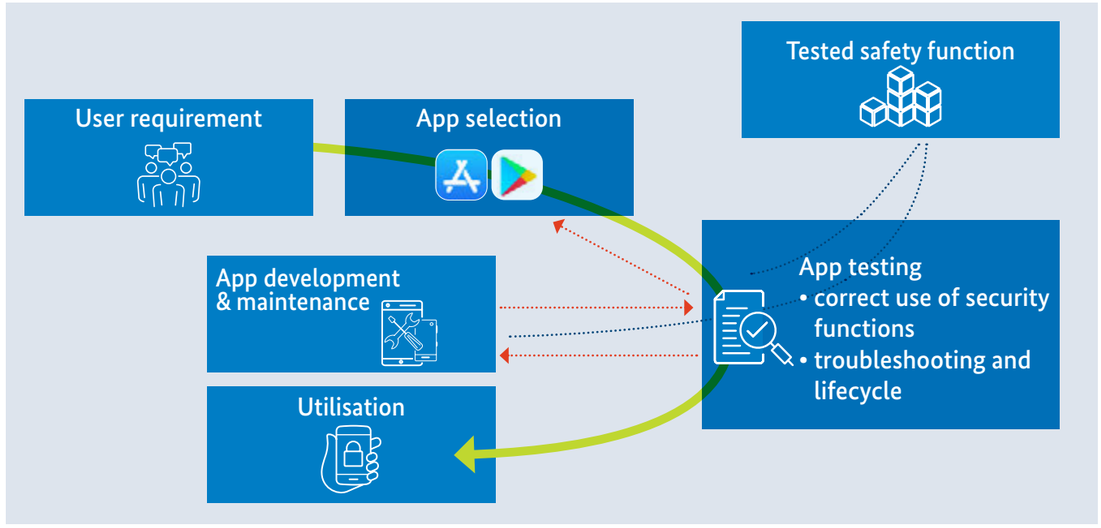


Figure 2: Inclusion of apps in the ecosystem

An Important Milestone for the Smart Grid

With the New Technical Guideline (TR) Communication Adapters, the BSI is Advancing the Transformation of the Energy Grid into a Secure Smart Grid.

By Michael Brehm and Dr Andreas Resch, Division Cyber Security for Digitization of the Energy Sector

With the publication of TR-03109-5 Communication Adapter, the BSI has reached a milestone for the secure communication of technical equipment to the communication Divison Smart-Meter-Gateway (SMGW). This makes it possible to connect controlable and sub-meter devices securely and interoperably.

The energy transition is leading to a sharp increase in the number of decentralised power-generation systems in the electricity grid. Not only photovoltaic plants (PV) and electricity storage systems with inverters are in vogue, but also load-variable consumption devices such as heat pumps or e-charging stations. In terms of grid stability, it is important to flexibly coordinate power generation and consumption. In the smart grid, stakeholders in the energy system are digitally interconnected – from power generation to transport, storage and distribution through to consumption. Against the backdrop of a high threat level, it is therefore more important than ever to protect the communicative connection of all parties concerned against cyber attacks.

The TR Communication Adapter published in December 2023 has now laid the foundation for the secure integration of generation and consumption systems into the smart grid. In addition to interconnecting these systems, it also enables consumption-measuring devices to be accessed via the secure SMGW infrastructure.

CONNECTION OF DEVICES TO SMGW ONLY POSSIBLE WITH BSI SPECIFICATIONS

The SMGW is the communication Divison of the intelligent metering system (iMSys). It connects the backend systems in the wide area network (WAN) with the locally installed measuring devices in the local metrological network (LMN) and also with the technical equipment in the home area network (HAN with HAN-CLS and HAN-CON). In principle, technical equipment can only be connected to the SMGW if it fulfils the interoperability and IT security requirements of the BSI. The TR formulates minimum requirements for the components in the HAN-CLS (so-called CLS components) that implement the functional scope of a communication adapter. Technical devices can be consumption and power generation devices, but also control devices for connecting new and existing systems or products for remote capturing of sensors.

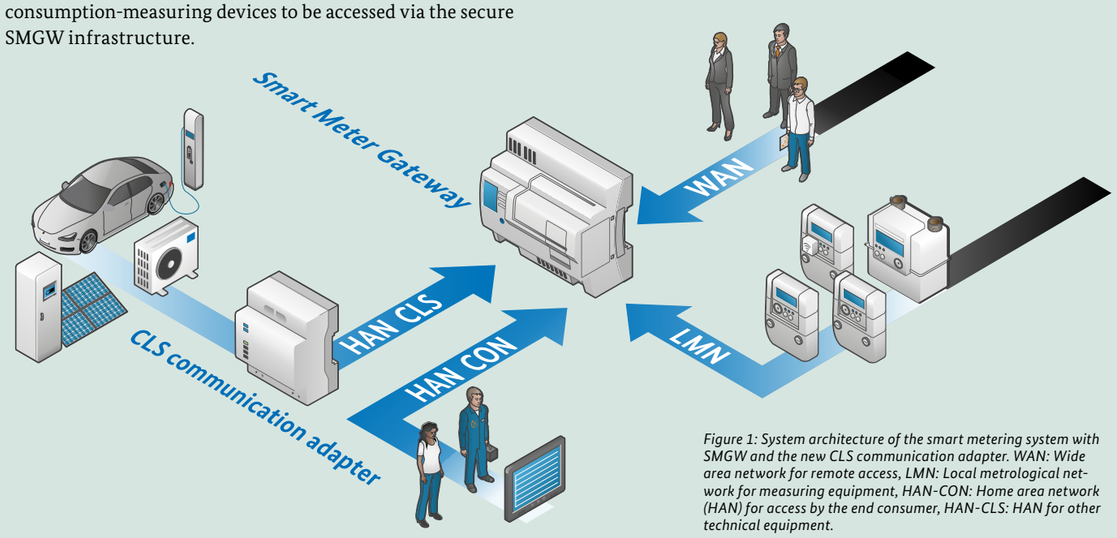


Figure 1: System architecture of the smart metering system with SMGW and the new CLS communication adapter. WAN: Wide area network for remote access, LMN: Local metrological network for measuring equipment, HAN-CON: Home area network (HAN) for access by the end consumer, HAN-CLS: HAN for other technical equipment.

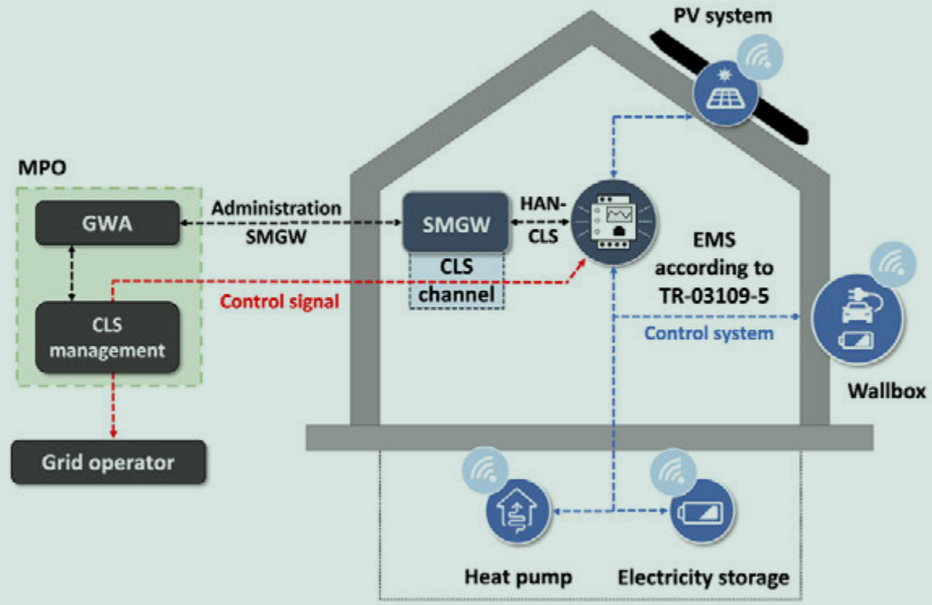


Figure 2: Example of the implementation of grid-orientated control via iMSys with SMGW and EMS. GWA: gateway administrator; MSB: metering point operator; EMS: energy management system as CLS component in accordance with TR-03109-5; red arrows: logical signalling path; black arrows: physical signalling path.

EXAMPLES OF SECURE APPLICATION

From 2025, the Metering Point Operation Act will require that consumption and power-generation facilities can be controlled securely and interoperably via the SMGW. Figure 2 illustrates how the energy management system (EMS) securely receives the control signal from a grid operator via the CLS channel of the SMGW. It evaluates it and controls the connected devices – exactly in the same way, as the specifications and stored parameters of the grid operator require. As a CLS component, it is certified by the BSI.

MINIMUM REQUIREMENTS OF THE TR COMMUNICATION ADAPTER

The TR defines security objectives and sets minimum requirements for the security performance of CLS components. It is primarily concerned with

- Interoperability requirements,
- the use of the CLS channel
- the implementation of firmware updates
- the keeping of a system time.

To use the CLS channel, it is necessary to establish a TLS connection with the SMGW. To make commissioning as easy as possible, the CLS components must be able to automatically integrate into the HAN-CLS network and use the services of the SMGW.

If there are connections to other networks that are not secured by the SMGW, the CLS components are not fully protected. The IT security requirements are primarily intended to prevent possible attacks on the CLS components.

APPLICATIONS FOR CERTIFICATION CAN BE SUBMITTED

The TR forms the basis for the implementation of certification procedures in accordance with the Technical Guideline and for the BSI's "Fixed-time cyber security certification" (BSZ).

A test specification and a product certification programme have been created for the certification in accordance with the Technical Guideline so that manufacturers can now submit corresponding certification applications.

In order to be able to establish certification in the new BSZ scope "Components in the HAN of the SMGW" (AIS-B SMGW HAN), the basic principles must be evaluated and tested in two pilot processes. Numerous manufacturers applied with their products for this. It is planned to open up the scope of certification to all manufacturers from the second half of the year once the pilot procedures have been completed.

HIGH ACCEPTANCE AND STRONG SUPPORT IN THE INDUSTRY

The TR Communication Adapter has met with a high level of acceptance and strong support from the energy industry. This became clear at the final hearing in the Gateway Standardisation Committee. The BSI had previously involved the industry in the development of the TR in several calls for comments and received valuable feedback. The guideline is considered a pioneer for important use cases in the energy industry. The BSI is thus actively shaping security in the smart grid and contributing directly to the success of the digitalisation of the energy sector. ■

Portal Network: Cybersecurity Around the Online Access Act

Advancing Administrative Digitalisation Consistently, Pragmatically and Securely

By Michael Bauer and Dr Thorsten Limböck, Division eID Solutions for Digital Administration, and Erik Mann and Eva Stützer, Division Inspection Systems for Official Documents

In 2017, the "Act to Improve Online Access to Administrative Services – Online Access Act (OZG)"[1] came into force. It obliges the federal and state governments to make their administrative services available electronically via administrative portals. An initial look at the working version of the technical guideline BSI TR 03172 makes it clear how IT security is to be guaranteed.

The interaction clarifies administrative portals can be improved in the future if they are linked to form an interoperable portal network. The aim is to ensure that an administrative service can be accessed from any portal. The portal network uses common central components to connect the individual components of the administration portals. The central components include, for example, the service accounts as a identification and authentication solution with a mailbox function and the "Portalverbund Online-Gateway" as a search engine for administrative services. The individual components of the administration portals are, in particular, online application services for the various administrative services.

FEDERAL AND STATE GOVERNMENTS HARMONISE GUIDELINES

"IT-Sicherheitsverordnung Portalverbund"[2] formulates IT security requirements for the components of the portal network. In addition to the security requirements from IT baseline protection, the Regulation specifies the BSI's technical guidelines in particular as the state of the art for ensuring IT security. The BSI Technical Guideline TR-03172 "Portal Network"[3] is currently being developed in coordination with the federal and state governments. The focus is on the security aspect of individual components – at the same time, the security of the entire portal network is being considered.

The first three documents (framework document and parts 3 and 4) are currently published in working versions and are briefly presented here: The BSI TR-03172 framework document provides basic information for people involved in the security of a portal network. It contains an introduction, explains the structure of a portal network and illustrates the interaction of the individual components using a sample application. A glossary explains the most important terms.

Part 3 "Online service" of the Technical Guideline lists requirements for web-based application services and assistants for administrative services. It primarily deals with functionalities that are necessary for online services in this context, such as authentication, session management or input validation. It also contains specifications for designing a secure architecture and for the intermediate storage and sending of applications.

An application routing service is required if several specialised authorities are connected to an online service and the specialised procedure responsible for the respective application must be determined within these authorities. The completed application is then sent to the determined procedure. The requirements for these processes are stated in Technical Guideline 03172-4 "Application routing".

FURTHER DOCUMENTS ON IMPORTANT COMPONENTS WILL FOLLOW

The portal network also includes other components that shallbe mapped in TR-03172 in the future. These include, for example, the data protection cockpit. In accordance with Section 10 OZG, it allows natural persons to track the exchange of their data between connected authorities, provided that this has taken place using the person's identification number (IDNr). If records of the exchange are available in the registers, a person receives an overview of which data from the register has been requested by another authority. In this way, more transparency can be achieved in the use of personal data.

The data protection cockpit is being developed under the leadership of the state of Bremen. The BSI is providing support with the security aspects and thus has the opportunity to draw up the associated TR-03172-2 in a practical manner and in parallel with the development process. Particular attention is paid to the protection of sensitive data, which may only be displayed to the person accessing it. For this reason, it is essential that the identity of the person making the enquiry can be determined beyond doubt during the registration process. Furthermore, it must be ensured that no personal data is stored in the data protection cockpit or can flow out.

Further documents on components such as the portal network online gateway or a payment service for paying fees will supplement TR-03172 in the future.

DIVERSITY OF IT SYSTEMS BECOMES A CHALLENGE

One challenge in the development of the technical guideline is the diverse landscape of IT systems that goes beyond the portal network. In parallel to the digitalisation of services for users, the administrative structures, including specialist procedures and registers, must also be designed to be securely digital. The BSI is supporting this implementation process as part of register modernisation[4]. The OZG Amendment Act takes into account the experience and findings from the implementation of the digitalisation of administrative services to date. For example, there are plans to strengthen the eID as a standard means of authentication, as well as a new and centralised seal service to apply and verify qualified electronic seals. Administrative digitisation is now seen as a permanent task. Simplified, accelerated and seamless communication with the administration can only be secure and trustworthy if information security is considered from the outset. ■

Technical Guideline:

https://www.bsi.bund.de/dok/tr-03172

1 https://www.gesetze-im-internet.de/ozg/BJNR313800017.html
2 https://www.gesetze-im-internet.de/itsiv-pv/BJNR001800022.html
3 https://www.bsi.bund.de/dok/tr-03172
4 https://www.gesetze-im-internet.de/regmog/BJNR059100021.html

The European Cyber Resilience Act – an Update

Europe Agrees on Rules for More Cybersecurity

by Anna Thurm, Market Surveillance Divison for Certified Service Providers and Products

In December 2023, after three months of negotiations, the European Commission, Council and Parliament reached an agreement on the Cyber Resilience Act (CRA), thereby concluding the so-called trilogue. After finalising the text, the Act was adopted by the European Parliament in March 2024 and is now awaiting approval by the Council

In September 2022, the European Commission published the draft of the CRA. The EU regulation aims to introduce horizontal – i.e. product category-independent – cybersecurity requirements for the protection of digital products over their entire life cycle for the first time.

AN UPGRADE FOR INFORMATION SECURITY

The new regulations will apply to connected or network enabled for which there are not already more extensive regulations, such as medical devices, motorised vehicles and civil aviation. It therefore also applies to software. Only open source software outside of commercial activities is explicitly excluded from the scope of application.

The regulation defines access requirements for the EU internal market and thus extends the scope of the already familiar CE mark. Once the CRA comes into force, this assurance of the safety of a product by the manufacturer will for the first time apply not only to safety, i.e. operational safety, but also to security, i.e. information security. In order to guarantee this, manufacturers now have new obligations that apply not only at the time of purchase, but also for the duration of the normal use of a product.

The CRA places requirements on manufacturers of products with digital elements as well as on the products themselves. This includes basic requirements for products such as security by design, security by default and ensuring the confidentiality and integrity of processed data. The CRA also includes requirements for the manufacturer to deal with vulnerabilities, e. g. the obligation to provide security updates over the entire life cycle of the product, to report and rectify vulnerabilities and to maintain a software bill of materials (SBOM). Comprehensive documentation for users on the product and contact options for reporting vulnerabilities are also required.

Some details of the regulation were still the subject of discussion in the trialogue. Compared to the draft published in 2022, the negotiations resulted in the following changes to the legal text, for example

- Clearly visible indication of the end of the support period on the product at the time of purchase
- Determination of the product's support period is done by the manufacturer, taking into account, among other things, reasonable user expectations and normal service life
- Reporting channels and deadlines for vulnerabilities
- Assignment of product categories to risk classes, renaming of risk classes
- Transition period until the start of application
- Specification of the exception for open source

These obligations apply not only to manufacturers, but also to importers or distributors, i.e. those who place products with digital elements on the EU internal market. Market surveillance authorities are set up in the individual member states, which can withdraw affected products from the market if the requirements are not met. There is also the threat of severe financial penalties.

SUPPORT FROM THE BSI TO IMPLEMENT THE REQUIREMENTS OF THE CRA

The transitional period from entry into force to the start of application of the EU regulation will be 36 months. Due to its horizontal scope, the CRA will be mandatory in its application for a large number of products with digital elements. It is advisable for manufacturers to prepare for the new market access requirements. It will take time and several cycles of experience to establish the necessary processes. In order to make the requirements of the CRA more tangible in advance, the BSI is developing a technical guideline in which the requirements for manufacturers and products with regard to cyber resilience are described clearly and specifically. A partial document with specifications on the scope, content and format of a software bill of materials was already made available in August 2023.

The BSI is also involved in standardisation. The EU Commission draws on the expertise of the European standardisation committees for many more specific requirements within the framework of the CRA, for example for product categories that are particularly worthy of protection. The BSI's experts are involved there in the secure design of consumer products. ■

Strengthening Cooperation and Cyber Resilience in Europe

Top-level Meeting fo European Cybersecurity Authorities in Munich in February

By Clarissa Wilkie, Division International Relations

At the invitation of the BSI, 26 directors of the European authorities responsible for cybersecurity came together to discuss current national, European and international challenges. This year's meeting focussed on the challenges posed by new EU legislation on cybersecurity, in particular the NIS 2 Directive. In the interests of a coherent approach across Europe, the participants discussed, among other things, how IT security incidents at multinational companies can be tackled together in future.

The central topic of the meeting on 15 February was European legislation relevant to cybersecurity. There was agreement that their efficient implementation and the avoidance of fragmentation are among the major challenges that the competent authorities can only overcome by working closely together. With this in mind, a joint declaration was drawn up focussing on the upcoming implementation of the NIS-2 Directive. At the same time, the declaration appeals to the EU legislator to give the member states sufficient time for efficient, effective and harmonised implementation of the legal acts before new legislative projects are initiated.

EUROPEAN COMMITMENT OF THE BSI

The BSI is continuously involved in relevant EU committees and working groups, such as the NIS Cooperation Group, in order to contribute its own experience from the KRITIS sector, for example. For the BSI, international cooperation is an essential success factor for improving cybersecurity in Germany and Europe. The Directors' Meeting, organised for the first time by the BSI in collaboration with the Munich Cyber Security Conference, has offered participants the opportunity to discuss strategic options for action in terms of European cooperation every year since 2020. The meetings are attended not only by representatives from the EU member states, but also from the four EFTA states of Iceland, Liechtenstein, Norway and Switzerland, as well as from the United Kingdom and the European Union Agency for Cybersecurity (ENISA).

IMPORTANT CONTRIBUTION TO THE NETWORKING OF AUTHORITIES

By organising the Cyber Security Directors' Meeting – the official title of the event – the BSI is making an important contribution to better networking between the authorities with national responsibility for cybersecurity. The great need for dialogue at this level is demonstrated by the decision of the Directors' Meeting to hold the event at least twice a year in future. A second meeting was already organised by the BSI's Belgian partner authority in Ghent in May 2024 as part of the EU Council Presidency. ■

BSI President Claudia Plattner (centre) hosted the event. The exchange focussed on strategic cyber-security issues.

A large number of directors accepted the BSI's invitation to Munich.

THE INTERNATIONAL COMMITMENT OF THE BSI

International cooperation has been an essential factor in improving cybersecurity for the BSI since it was founded more than 30 years ago. In addition to its national role as the federal cybersecurity authority, the BSI aims to help shape cybersecurity internationally and to strengthen its own tech nological assessment capabilities. In order to adequately fulfil its responsibility in this regard, the BSI is continuously intensifying and expanding its relationships with authorities, organisations, companies and stakeholders in science and civil society worldwide. The work in various expert committees on information and cybersecurity in the EU, NATO and international context is an essential part of the BSI's international commitment.

European Perspective(s) for Strong Digital Consumer Protection

Inspiring Exchange at the First European Symposium “Cybersecurity for Europe: Integrating the Consumer Perspective” in Dresden

By Kristina Unverricht and Dr Jörg Hübner, Division Basic Issues of Digital Consumer Protection and Cooperations

At the beginning of February 2024, the BSI organised the European symposium “Cybersecurity for Europe: Integrating the Consumer Perspective” for the first time. Representatives of European cybersecurity organisations, consumer protection organisations and the European Commission took the opportunity to develop ideas and approaches for improving digital consumer protection.

The symposium focussed on the challenges of digital consumer protection and – in view of cross-border cybercrime – the importance of a common European perspective. For the BSI, three key points are important for the future shaping of digital consumer protection in Germany:

- We ensure that IT devices and software come onto the market securely: With the IT security label, the BSI has already implemented an effective tool for improving product security. As security by design is firmly anchored in digital consumer protection, the BSI therefore also sees itself as responsible for assuming the market surveillance function of the Cyber Resilience Act.

- The BSI is being developed into the central German centre for the protection of people online: Because diverging standards within Europe represent a weakening of IT security for users in the long term, we are actively expanding the networking of important stakeholders on the continent. In this way, we are promoting secure, cross-border digitalisation.

- Digital consumer protection should not end with information services for consumers, but should underpin these with active protective measures: In addition to the important educational work, it is necessary to identify technical means to prevent damage and cyber attacks as they occur. The principle of human-centred design will be at the heart of the design of measures.

CONFIDENT CONSUMERS

The questions of what the necessary framework conditions for successful protection in digitally networked everyday life should look like and how the consumer protection perspective can be integrated into European cyber security regulation provided material for discussion. The discussion was underpinned by practice-oriented presentations on the interests and requirements of consumers with regard to their cyber security.

Left: Panel discussion on the joint perspectives of European digital consumer protection, from left to right: Lars Bartsch (BSI), Ruben Verstraete (Directorate General for Economic Inspection, Inspector International Coordination, FPS Economy, Brussels), Dr Karen Renaud (Strathclyde University, Glasgow), Claudio Teixeira (Legal Officer – Digital and Consumer Rights, The European Consumer Organisation BEUC), Kristina Unverricht (BSI)

The speakers put forward the following propositions for effective digital consumer protection in the future:

- Digital consumer protection protects against cyber threats in the digital space without restricting the sovereignty of consumers. Basic protection must be ensured through minimum security requirements for all networked products and services.

- Digital consumer protection includes all consumer groups. This applies in particular to the requirements of vulnerable consumers. Appropriate participation formats are needed. The responsibility for cybersecurity must not be imposed on consumers. Developments in digitalisation and technological innovations must not be at the expense of consumers, but must be designed to be secure from the outset.

- Digital consumer protection starts at multiple levels: particularly in (user-centred) product and service design, but also in marketplaces for digital products. Europe needs new strategies and tools for effective and efficient implementation.

- Efficient digital consumer protection is achieved through a cooperative approach, i.e. by bringing in the respective expertise of the organisations and stakeholders involved.

The symposium served as a platform for networking and exchange, but also for knowledge transfer in order to continue working together on the challenges for strong European digital consumer protection. The successful event format will provide a regular platform for dialogue in the future. ■

Dr Karen Renaud from Strathclyde University (Glasgow) gave insights into “human-centred security aspects” to improve digital consumer protection

András Zsigmond, Legal Coordinator of the Consumer Product Safety Divison of the European Commission, spoke about the new EU product safety regulation GPSR

Further information on digital consumer protection:

www.bsi.bund.de/VerbraucherInnen

Social Engineering: Protection against AI-supported Cyber Attacks

Artificial Intelligence Takes Cyber Attacks to a New Level

By Jan Lammertz, Division Cyber Security for Society and Citizens

Machine-generated videos, images, texts and voices are now widespread phenomena. If people are deceived, e. g. with the help of such generated imitations, into trusting attackers and granting them access to data, for example, this is known as social engineering. By using artificial intelligence (AI), cyber criminals can sometimes make these manipulative attacks more efficient and effective.

We take a look at the dynamics of this phenomenon, the influence of AI on social engineering and the challenges and protection options for users.

Artificial intelligence can take digital deception to another level and this is precisely what is exploited in social engineering: Cybercriminals try to manipulate human behaviour. A new dimension has been reached through the use of AI. “Social engineering 2.0” is characterised by even more personalised and sophisticated attacks in which AI is used to create fake videos, images, voices or personality profiles to deceive people. The aim is to gain access to information, systems or networks. AI now enables cybercriminals to carry out more convincing attacks more efficiently and to pressure their victims into rash actions.

Using machine learning, AI can increasently imitate human behaviour and orchestrate personalised attacks faster. These techniques make it more difficult to detect fraudulent activity as the attacks are based on the individual behaviour patterns of the target.

These methods are constantly evolving and cybercriminals are trying to stay ahead of security measures. This is why sensitisation, training and regular security checks are crucial to protect against social engineering attacks.

WE BRIEFLY PRESENT SPECIAL FORMS OF SOCIAL ENGINEERING:

Spear phishing:
Cybercriminals target their phishing attacks at a specific person or organisation by using personalised information to gain trust.

Whaling:
Similar in design to spear phishing, but whaling targets high-level executives or important people.

Vishing (voice phishing):
Cybercriminals use phone calls to impersonate a legitimate person or organisation to obtain sensitive information.

Social media exploitation:
Through the (automated) analysis of social media profiles, cybercriminals collect personal information to target individuals.

Deepfakes:
Artificial intelligence is used to create fake videos or audio recordings to trick people into certain actions or to spread fake news, for example.

IoT exploitation:
Cybercriminals exploit vulnerabilities in networked devices and the Internet of Things (IoT) to gain access to personal or business networks.

HOW CAN INTERNET USERS PROTECT THEMSELVES AGAINST SOCIAL ENGINEERING?

Social engineering with AI-supported attacks pose particular challenges for users: The increasing difficulty in distinguishing between real and fake content requires improved security awareness. As attacks become more personalised and subtle, people need to learn to be more vigilant in their digital lives when faced with unusual requests or suspicious activity.

In order to protect themselves against these sophisticated attacks, users should strengthen their security precautions. For example, the use of promptly installed software updates, always up-to-date antivirus programs and firewalls provide a sensible basis for protection against unauthorised access.

In addition, a healthy scepticism towards unexpected digital messages and requests makes sense. For example, you can effectively protect yourself against attacks by trying to reach the supposed sender of a message on a different channel and verifying the request. Anyone affected by such an attack should collect evidence via screenshots and report the case to the police.

HOW CAN THE USE OF TECHNOLOGY PROTECT PEOPLE?

Cyber criminals and cyber defence systems are in a constant race that often determines the success or failure of a cyber attack. On the one hand, AI gives cyber criminals the opportunity to develop effective methods of social engineering. On the other hand, machine learning tools can be used in return, e. g. to recognise AI-generated phishing attempts.

The primary goal of such AI-supported detection software is to identify and block certain patterns of phishing content in messages or on websites based on training data. Such filters can be integrated into web browsers, email services or IT networks to keep an eye out for suspicious activities in real time and, if necessary, raise the alarm.

INCREASED RISK AWARENESS IS BASICLY IMPORTANT

Social engineering, supported by artificial intelligence, therefore requires continuous adaptation of security practices and constant vigilance. User must be aware that the attack landscape has become much more diverse and insecure due to the use of AI by cyber criminals. Technical measures, increased risk awareness and basic caution on the internet can help to protect the digital identity and personal data more effectively. ■

Further information:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Soziale-Netzwerke/Sichere-Verwendung/sichere-verwendung_node.html

Tips for Digital Family Life

How Parents Can Support and Protect Their Children Online

By Larissa Hänzgen, Division Cyber Security for Society and Citizens

Digital media is now a natural part of family life. Computers, laptops, games consoles, smart speakers and, above all, smartphones and tablets are often part of everyday life. Even the youngest children enjoy using them – often unaccompanied. Most of these devices provide easy and almost unlimited access to the web. Without the appropriate settings, this can be dangerous and pose security risks.

BASIC IT PROTECTION FOR CHILDREN AND YOUNG PEOPLE

Anyone who works with children and young people faces the challenge of responsible use of digital media and creating a safe online environment. Fortunately, there are technical safeguards are available to protect young media users from potential online dangers. Basic parental controls are usually built into modern operating systems, but they need to be activated and adapted to the individual needs. The following basic tips from the BSI will help you to establish the foundations for a safe digital family life.

1. SET UP A SEPARATE USER ACCOUNT FOR EACH CHILD

Setting up a separate user account without administrator rights on the PC is an important first step. You can add a user under Account in the computer settings. By setting up a separate account, you can, for example, restrict access to sensitive data and settings on the main account. This can help prevent malware from taking advantage of administrator privileges to, for example, infect or damage files on the system.

Risks for children and teens on the internet

Protection against malware

Young users in particular are easily tempted to click on icons and links that promise exciting content or free games. This makes it easy for them to fall into the trap of cybercriminals. Opening infected emails or other electronic messages, but also simply by visiting websites, can infect computers with malicious programmes such as viruses, worms or Trojans.

The dangers from spam and phishing

Children and teens are also confronted with spam or fraudulent phishing messages via email, messenger or social networks. In addition to traditional advertising, these messages may contain malware or links to infected websites, or may be are aimed at obtaining personal and sensitive information.

Disclosure of personal data

Social media thrives on the exchange of information, photos of friends or videos from holidays. But there are risks associated with this wealth of information Sensitive information such as name, date of birth, phone number, address or even account and bank details should never be shared.

Cyberbullying is on the rise

It‘s not just cybercriminals who are after personal data. Insults and exclusion are increasingly being carried out online. Perpetrators use social networks or messengers to expose, harass or insult their victims. They then threaten to distribute or publish private pictures, for example.

Unsuitable content accessible for children online

While there is a lot of useful contenton the internet, there is also inappropriate content that is just a click away, especially for children. Online games that glorify violence and racist or pornographic statements and depictions are just a few examples. Risks also lurk in seemingly harmless online services such as messengers and social media.

2. USE AN ANTIVIRUS PROGRAMME

Unsafe downloads, such as games, can install malicious software on your child‘s computer. An antivirus program detects and blocks malware and security threats. Most operating systems come with an antivirus program built in. Enable it the software in the computer‘s security settings and keep it up to date with automatic updates.

3. CHECK THE FIREWALL

Most operating systems have a built-in firewall. Check your yoursystem settings to see if this is enabled . If not, activate the firewall and adjust it to your individual needs in order to protect your system and your children‘s system from unauthorised access and potential external threats. You can also configure the firewall to only allow certain programs and applications to access the Internet. This minimises the risk of children and teens downloading harmful applications, programs or games.

4. USE A ROUTER WITH PARENTAL CONTROL SETTINGS

Modern routers can control Internet access for each device connected tothe home network. Each device is assigned an access profile via the router, which can be used to limit online time, enable or restrict network applications, or block certain websites can be blocked. The settings can be changed on all the children's and teenagers' devices, while the parents' devices retain full access. You can also secure your wireless network with a strong password to prevent unauthorised access and maintain control over who can access the internet.

5. USE A CHILDREN'S SEARCH ENGINE

There are special children's search engines to help children search online safely. These show only child-friendly and even editorially filtered content. In addition, most children's search engines also suppress adverts or (fake) pop-ups. This minimises the risk of children being directed to fake websites, downloading malware or seeing inappropriate content. Once you have chosen a search engine, set it as your browser's home page.. Most browsers also offer parental controls in the form of browser extensions that can be used to block individual websites.

6. SET TIME LIMITS

This feature is often built into in parental control software, but can also be found in operating systems. Time limits allow you to set how long your children can use their devices and be online. It's not just about limiting screen time for the whole week, but also limiting it to different times of the day to prevent children from being online late at night or unsupervised. Some operating systems and software solutions also allow you to set limits for specific games and apps.

7. RAISE AWARENESS OF GOOD ACCOUNT PROTECTION AT AN EARLY STAGE

Once children and teenagers are online, they too can become victims of phishing attacks. Teach them the importance of strong passwords and how to create and manage them, for example using a password manager. Where possible, set up two-factor authentication. Children should also know that they should never share passwords with others or give out personal information to strangers.

8. TALK ABOUT RISKS AND SAFEGUARDS ONLINE

For children to become confident and empowered online users, they need to be supported and encouraged to use of digital media critically and responsibly. An open and trusting basis for dialogue is just as important as technical safeguards.. Talk to your children as equals, show interest and understanding – even in difficult situations. Banning, punishing or taking away devices can make your children less likely to confide in you.

9. RESPECT THE PRIVACY OF CHILDREN AND YOUNG PEOPLE

According to Article 16 of the UN Convention on the Rights of the Child, children and young people have a right to privacy. Adapt the parental control software to the age of the child, inform them about the settings stored and maintain an appropriate balance between privacy and technical protection measures.

TIP:

Many modern operating systems come with built-in parental controls that can be adjusted to suit different needs and age. There is also a wide range of third-party parental control software available. These features and programmes allow parents to restrict access to certain websites, apps and content, and to control online activities.

Further informationen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Sicher-im-digitalen-Schulalltag/digitaler-schulalltag_node.html

Eight tips for everyday digital family life:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Wegweiser_kompakt_digitaler_Familienalltag.html

Step by step to parental control settings for apps, games & co.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/SfS-Anleitung_Jugendschutzeinstellungen_Apps_Spiele_Co.html

Order your BSI Magazine

Federal Office for Information Security

Federal Office for
Information Security (BSI)
Division Public Relations

P.O. Box 20 03 63
53133 Bonn
Phone +49 (0) 228 99 9582 0
Fax +49 (0) 228 99 9582-5455
Email: bsi-magazin@bsi.bund.de

Twice a year, the BSI Magazine "Security in focus" offers insight into national and international cybersecurity, digital society and IT security in practice.

You can receive the latest editions directly by mail following publication in June and in December by subscribing to the distribution list with the form below.

I would like to subscribe to the following BSI publication:

☐ BSI Magazine "Security in focus" (2/year, print)
☐ The State of IT Security in Germany (1/year, print)

Last name, first name

Organisation

Street, House No.

Postal code, City

Email

Data protection consent:
I consent to my aforementioned personal data being used, electronically stored and processed by the BSI as the responsible body for the dispatch or transmission of the aforementioned publications. No data will be given to third parties without consent.

Date/Signature:

The Federal Office for Information Security, PO Box 20 03 63, 53133 Bonn, Germany, is responsible for processing your aforementioned personal data. The data you provide will only be used to manage the sending or transmission of the information you have consented to above. You may revoke this consent at any time. Simply send an email to bsi-magazin@bsi.bund.de. Revoking consent does not affect the legality of prior processing done before revocation. For more information on how we process your personal data and what rights you are entitled to, please refer to the "Privacy policy" attached for ordering BSI publications. Simply send in the form by fax or email:
Fax: +49 (0) 228 99 9582 5455 | Email: bsi-magazin@bsi.bund.de

Or you can register directly online: https://www.bsi.bund.de/EN/BSI-Magazine

If you no longer wish to receive BSI publications, simply send us an email to:
bsi-magazin@bsi.bund.de.

Privacy policy
https://www.bsi.bund.de/EN/Service/Datenschutz/datenschutz_node.html

Legal Notice

Published by:	Federal Office for Information Security (BSI) 53175 Bonn
Source:	Federal Office for Information Security Division Public Relations Godesberger Allee 87 53175 Bonn Phone: +49 (0) 228 999582-0 E-mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de/EN
Last updated	June 2024
Content and editing:	Katrin Alberts, Sonia Golás, Brigitte Hoffmann, Mark Schulz, Bundesamt für Sicherheit in der Informationstechnik; KOMPAKTMEDIEN, Agentur für Kommunikation GmbH, Torstraße 49, 10119 Berlin, www.kompaktmedien.de
Concept and design:	Federal Office for Information Security (BSI)
Printed by:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3, 96277 Schneckenlohe, www.ak-druck-medien.de
Item number:	BSI-Mag24/717-1e
Image credits:	Cover: BSI; p. 3: © BMI/Henning Schacht; p. 4 – 5 (left to right): AdobeStock © ipopba; BSI; BSI; AdobeStock © Limitless Visions; AdobeStock © MNStudio; AdobeStock © Summit Art Creation und AdobeStock © Inactive; p. 6 – 7: © BSI; p. 9: AdobeStock © ipopba; p. 10 – 11 (left to right): AdobeStock © Aon Khanisorn; AdobeStock © phaisarnwong; AdobeStock © New Africa; AdobeStock © visoot; AdobeStock © Donson/peopleimages.com; AdobeStock © standret; AdobeStock © Alessandro Rizzi; AdobeStock © olga_demina; AdobeStock © chokniti; AdobeStock © Климов Максим; AdobeStock © Gorodenkoff; AdobeStock © Syntetic Dreams; AdobeStock © likoper; p. 12 – 13: © BSI; p. 14 – 15 (above): AdobeStock © Sergey Nivens und AdobeStock © DP, (bottom): © BSI; p. 16 – 17: AdobeStock © Sascha; p. 18: © BSI/bundesfoto Bastian Geza Aschoff; p. 19: © BSI/bundesfoto Bastian Geza Aschoff; p.: 21: AdobeStock © Genestro; p. 22: © BSI/bundesfoto Bernd Lammel; p. 23 (above and right): © BSI/bundesfoto Bernd Lammel, (bottom left and midle): © BSI/bundesfoto Bastian Geza Aschoff; p. 24 – 25: AdobeStock © xyz; p. 26: © Matthias Rietschel; p. 27: © BSI und privat; p. 29: © BSI; p. 15: © BSI; p. 32: © Markus J. Feger; p. 33: AdobeStock © Vikky Mir; © BSI, AdobeStock © The KonG, © BSI, © Fotolia, © BSI, © BSI/bundesfoto Uwe Völkner; p. 34: privat, privat; p. 36 – 39: AdobeStock © nongkran_ch, p. 38: © Markus J.Feger; p. 40 – 41: AdobeStock © Limitless Visions, © BSI, © BSI; p. 42: © BSI; p. 43: © BSI; p. 45: AdobeStock © vegefox.com; p. 46 – 47: AdobeStock © nosorogua, AdobeStock © MNStudio;p. 49: © BSI; p. 50 – 51: AdobeStock © Natasa Tatarin, © BSI; p. 52: AdobeStock © David Santos Mendoza; P. 53: AdobeStock © Summit Art Creations und AdobeStock © Inactive; p. 54 (above): AdobeStock © musmellow, (bottom): AdobeStock © Mariia Korneeva; p. 55 – 56 (traffic signs): AobeStock © Dejan Jovanovic; p. 57: © BSI

The BSI Magazine is published bi-annually. It is part of the Federal Office for Information Security's public relations work.

It is provided free of charge and is not intended for sale.

Scan the QR code for the digital version of the BSI Magazine

www.bsi.bund.de/EN/BSI-Magazine

Follow us:

ICH HAB NICHTS GEMACHT!

Schützen Sie Ihre smarten Geräte vor Schwierigkeiten. Wir helfen Ihnen dabei: einfachabsichern.de

Bundesamt für Sicherheit in der Informationstechnik

#einfachaBSIchern