In Focus: Artificial Intelligence

Security in focus

IT Security in Practice
Cyber Security for Local Authorities: The WiBA Project

Cyber Security
CERT-Bund: Proven Point of Contact Centre and Partner

The BSI
New Test Lab for 5G Networks at the BSI Site in Freital
Dear reader,

We assess the significance of a topic for our society by where it is being discussed. Artificial intelligence is now being covered not only in industry publications but also in daily newspapers and even on television. The opportunities and risks of this key technology have become a topic of conversation in workplaces, schoolyards and living rooms, as people of all ages use it – whether it is language assistance programmes for schoolwork or driver assistance systems for increased safety and comfort while driving. We are now making sure that cyber security also takes a top spot on the agenda. After all, the cyber security of this key technology must keep pace and be integrated into our everyday lives, into business products and into the processes of public authorities alike. The aim is to increase cyber resilience substantially so that we can withstand attacks and recover from them quickly.

To achieve this, it is worth looking at our focus on artificial intelligence. We report on how, at the BSI, we examine threat scenarios for quantum-assisted machine learning or cooperate with external experts in projects on AI security in cars. In an interview, two experts from the media supervisory authority discuss the AI tool KIVI and how it helps to detect offences against the child protection or human dignity.

Reading the BSI magazine makes it clear that we are by no means acting alone, but are cooperating in all directions, networking and connecting with others and bringing many stakeholders together. We are facing a nationwide task that requires consistent cooperation between politics, business, and society for its fulfilment. This is evident in our specialist article on the necessity of global security requirements for satellites as well as in the report on the symposium of German-speaking security authorities in Luxembourg on the topic of digital administration.

The high-level discussion between the Chairpersons of the Management Board of the European Union Agency for Cybersecurity (ENISA) also focusses on the need to coordinate and support each other across all borders. This networking concept is systematic. I am convinced that only through cooperation between politics, business and science can we strategically deploy our technological expertise and create a cyber market in Germany. When the federal and state governments work together, we can advance digitalisation. When the EU states pull together, we can shape cyber security pragmatically.

Germany must see itself as a cyber nation. This way, we can build the necessary resilience to counter the very real threat situation in the cyber area effectively. The BSI is ready to act as an enabler, partner and helper in building Germany as a cyber nation.

With this in mind, I wish you an exciting read.

Kind regards
Yours

Claudia Plattner
President of the Federal Office for Information Security
BSI and the State of Saxony-Anhalt Sign Cooperation Agreement

The BSI and the state of Saxony-Anhalt, represented by the Ministry of Infrastructure and Digital Affairs, have signed a cooperation agreement. This agreement concretises the previous collaboration in a total of nine specific areas of cooperation and defines priorities for the years in the future. The focus includes joint awareness-raising measures, a continued close and trusting exchange of cyber security information and mutual job shadowing. BSI Vice President Dr Gerhard Schabhüser said on the occasion of the signing: “The secure design of digitalisation is a particular concern of mine and I am convinced that it can only be successful if the federal and state governments work together. We have a long-standing partnership with the state of Saxony-Anhalt, which we are reaffirming with this step. Together, we are establishing a binding framework for bilateral cooperation. We look forward to working with the state of Saxony-Anhalt to further advance the topic of cyber security in Germany.” With the cooperation agreements, the BSI is continuously deepening the cooperation between the federal government and the federal states.

Further information:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht_Zero_Trust.html

A Look at the Boardroom: Publication Series Management Blitzlicht Launched

With its new publication series Management Blitzlicht, the BSI provides quick and compact information on current cyber security topics for company management.

The first issues have been published on the topics of cyber supply chain risk management and zero trust architectures. The management flashlight “Zero Trust: A holistic security approach”, for example, describes the basics of the Zero Trust approach and shows the seven steps required to successfully implement Zero Trust.

Further information:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht_Zero_Trust.html

The first graduates of the three-year “Digital Administration and Cyber Security” (DACS) degree programme have successfully completed their final exams. Four semesters of theory at the Federal University of Applied Sciences and two practical semesters in various areas at the BSI have prepared the young specialists for a job in cyber security. BSI President Claudia Plattner is delighted with the new colleagues: “Cyber security in Germany needs digital talent and the BSI has incredibly exciting jobs. The DACS degree programme therefore offers an absolute win-win situation for everyone involved. I am delighted that we can now welcome the first graduates to the BSI, who will continue to raise the level of cyber security in Germany with a dedicated team.”
Cyber Supply Chain Security – Importance, Content and Risks at a Glance

The Increasing Digitalisation of Supply Chains Harbours both Opportunities and Risks

By Salabil Hamadache and Raphael Miether, Division Cooperation with Manufacturers and Service Providers

Executives are concerned about vulnerabilities in their supply chain – and rightly so: according to the World Economic Forum’s Global Cybersecurity Outlook 2022, almost 40 per cent of respondents said they had been negatively affected by a cyber security incident involving third-party vendors or suppliers. 58 percent of CEOs considered their business partners and suppliers to be less resilient than their own organisation.

Today’s supply chains are widely ramified, globally networked systems in which institutions from both the public and private sectors work closely together. These include buyers, suppliers, developers, system integrators, service providers and other professionals from a wide range of sectors who work together to research, develop, manufacture, procure, deliver, integrate and use or manage products and services in a variety of ways. Cyber security plays a central role as these interactions are shaped and influenced by a wide range of technologies, regulatory frameworks and strategic approaches to ensure the integrity and security of these global supply chains. Securing such complex systems is an enormous challenge and requires holistic security concepts.

PAINFUL EXPERIENCES

One of the most prominent supply chain attacks to date is the attack on Solarwinds’ Orion network monitoring tool. Attackers succeeded in gaining access to the company’s build system and infiltrating malicious code over an extended period of time, which was then distributed to Solarwinds’ customers in the form of updates. The attack was mainly used for espionage and thus remained far below the actual damage potential. The complexity and impact of the attack are nevertheless considerable. The modified update was delivered to 18,000 users, including US authorities such as the Treasury Department and the National Nuclear Security Administration (NNSA). The attack is still considered a textbook version of an advanced persistent threat attack. Another well-known example is “log4shell”, a vulnerability in the popular Java logging framework log4j. The vulnerability allowed attackers to execute arbitrary code on the affected systems. The widespread use of the open source framework, which was a component of many products from well-known manufacturers, was particularly problematic. This incident also shows that the lack of transparency in software supply chains can lead to serious security incidents.

REGULATORY REQUIREMENTS

Politicians are responding to the situation and addressing the issue of supply chain security in two upcoming regulations. Under Article 21 of the NIS 2 Directive and Section 30 of the Implementation Act, essential and important institutions are required to take appropriate and proportionate technical, operational, and organisational measures for risk management in the area of cyber security in accordance with the “all hazards approach”. Specifically, companies that fall within the scope of application are required to establish a cyber supply chain risk management (C-SCRM) system. In order to be able to set up a functioning C-SCRM, a large number of processes are required which, among other things, bring the necessary transparency to the supply chain, such as the establishment of a supplier register and the operation of IT asset management. Furthermore, factors such as the cyber security practices of the supplying companies must be taken into account for a corresponding risk assessment. The review and expansion of existing contracts is a logical consequence here in order to fulfil the requirements of the NIS 2 directive.

Another EU regulatory project is the Cyber Resilience Act (CRA). This is intended to create a standardised legal framework for the entire EU internal market in the future. It will define IT security requirements on all products with digital elements that are placed on the EU market. Minimal IT security requirements must be met by almost all products with digital elements – from smart home devices to entire operating systems. The requirements will take into account security throughout the entire product cycle (planning, design, development, manufacture, delivery, maintenance), including the use of third-party components.

In addition to the planned legislation, certain sectors are already subject to supply chain security requirements. For example, the financial sector is regulated by the Digital Operations Resilience Act (DORA), which sets out requirements for the management of ICT third-party risks under Chapter V. The Radio Equipment Directive (RED), which is implemented here in Germany by the Radio Equipment Act, regulates the supply chains of radio equipment made available on the European market.
ECONOMIC ASPECTS
With the onset of the coronavirus pandemic, the relevance of economic aspects such as product availability and extended delivery times became apparent. The semiconductor industry in particular had to contend with severe supply bottlenecks. The Russian war against Ukraine also exacerbated the situation, as supply routes for noble gases required for semiconductor production were cut off. This situation poses an indirect risk for cyber security, as suppliers need to be switched – possibly to less trustworthy suppliers who open up new attack vectors, for example through counterfeiting. In order to minimise this risk and at the same time strengthen Europe’s digital sovereignty, the European Commission wants to double the European market share in the semiconductor sector to 20 percent by 2030 with the help of the European Chip Act.

NEW APPROACHES PAVE THE WAY FOR INCREASED SUPPLY CHAIN SECURITY
Supply chain security is complex and requires a holistic approach. In principle, there is no shortage of technical solutions. However, these alone are not enough to secure the supply chain. They should be viewed much more as tools: In the area of software supply chains, a software bill of material (see also article on p. 12) increases transparency. The use of machine-readable security advisories – as described in the Common Security Advisory Framework (CSAF) – also significantly shortens the response time to a known security vulnerability. However, supply chain security can only be guaranteed with the help of holistic security concepts. Tried and tested measures include IT asset management, cyber supply chain risk management (C-SCRM) and appropriate attention to this issue in awareness measures. These measures will become mandatory for many companies as a result of the upcoming regulations.

The BSI provides support with numerous offers such as the Cyber Risk Check, which enables small and medium sized enterprises (SMEs) to determine their own IT security level. It also shows which specific measures should be implemented. As SMEs make up a large part of supply chains, but at the same time tend to have smaller budgets for cyber security, this help is essential.

Another important element is the Technical Guideline TR-03183-2, which describes the requirements for a Software Bill of Materials. Not only are SBOMs a requirement of the CRA, they are also the only way to share information about dependencies in software components interoperably across company boundaries.

Supply chain security must be a top priority. This is why the first issue of the BSI’s “Management Blitzlicht”, a new format for the boardroom, describes how to set up an effective C-SCRM. The Alliance for Cyber Security’s handbook “Managing Cyber Risks” provides more details. As supply chain security affects almost all areas of a company, the necessary management attention and the provision of the required resources are an essential prerequisite.

Counterfeiting, especially known in the semiconductor sector, refers to the illegal production and distribution of counterfeit components that are sold as genuine products but may be inferior or even harmful.

Effective cyber supply chain risk management in 5 steps
The following 5 steps will help you to establish effective cyber supply chain risk management in order to respond appropriately to threats in the supply chain:

1. Aggregate expertise – Identify all employees related to the supply chain
2. Create standards – Develop policies, strategies and processes to address supply chain risks
3. Monitor and document assets – Make sure you know what hardware, software and services your company purchases and uses and from whom
4. Maintain contacts with suppliers and service providers – Gain a deeper understanding of your supply chain and suppliers
5. Review actions – Evaluate the effectiveness of your C-SCRM on a regular basis
More Security in the Supply Chain because of SBOM

A Software Bill of Materials (SBOM) Documents Components of Software Products and thus Helps to Uncover Vulnerabilities

By Anna Thurm, Division Market Surveillance of certified Service Providers and Products

Both commercial and free software components of products are listed in an SBOM. The software parts list makes dependencies on third-party components transparent and thus helps manufacturers, security researchers and professional users to monitor vulnerabilities.

WHAT IS AN SBOM?

A software bill of materials is a list of software components. It specifies which proprietary or third-party components (e.g. libraries) are used in the software. As almost always many different sources and components are used in the software development process, SBOMs are an important instrument for transparent visualisation of the software supply chain. An SBOM is therefore comparable to a list of ingredients for a dish. It is created automatically and is available as a machine-readable file.

USE OF SBOMs

If information about a vulnerability in a software or software library becomes known, manufacturers, operators and administrators are faced with the difficult task of finding out whether the software they produce or operate is affected by this vulnerability. With an SBOM, they have a list of the components used at their disposal and can therefore check more easily whether there is a need for action in their case. To do this, the product’s component list is matched with information on component vulnerabilities from vulnerability databases.

DIFFERENT FORMS OF AN SBOM

An SBOM is particularly informative if the listed components of the described software are broken down into their constituent parts. This also makes indirect dependencies across several levels transparent. SBOMs can therefore have a different level of detail and be characterised accordingly. They are also classified according to the stage of software development at which they were created, e.g. on the basis of the source code used (source SBOM) or as part of the build process (build SBOM).

BSI recommendations for SBOMs

In August 2023, the BSI published the Technical Guideline TR-03183-2 with formal and technical specifications for SBOMs as a guide. TR-03183-2 defines, for example, the required data fields, the required scope and the possible formats. These requirements are currently only recommendations and are intended to provide guidance and prepare for possible requirements from the EU Commission.

HISTORY OF THE SBOM

Originally, SBOMs were used to obtain an overview of the various licences of the integrated software components. With the added benefit for security in the software supply chain, SBOMs have also found their way into legal requirements. Executive Order 14028 of 2021 requires an SBOM for software purchased by the US government. Such an SBOM must meet the requirements of the National Telecommunications and Information Administration (NTIA), which were published under the title “The Minimum Elements For a Software Bill of Materials (SBOM)”.

FUTURE OF SBOM

SBOMs are one of the central requirements of the European Cyber Resilience Act (CRA). This has been available as a draft from the EU Commission since September 2022 and is currently in the legislative process. Manufacturers of products with digital elements are to be obliged to maintain an SBOM for vulnerability management. However, publication of the SBOM is not required. It only has to be submitted to the market surveillance authority on request.

WHAT FORMATS ARE THERE FOR SBOM?

There are different formats for representation and distribution of an SBOM. The most widely used are SPDX and CycloneDX. Essential information, e.g. the data fields required by the NTIA or in the BSI Technical Guideline, can be represented in both formats. However, if the full scope of the possible content of the respective format is utilised, they cannot be converted into each other completely loss-free.

VULNERABILITY INFORMATION AND SBOMs

A SBOM itself does not contain any information on vulnerabilities or their exploitability. The list does not indicate whether and to what extent a vulnerability in a software component exposes a risk to the product described by the SBOM. This requires further information about the specific vulnerability, for example by means of vulnerability information (so-called security advisories) in the Common Security Advisory Framework (CSAF) or Vulnerability Explotability eXchange (VEX) formats.

Further information:

https://www.bsi.bund.de/de/TRA-03183
Prevention and Response

CERT-Bund: Proven Contact Point and Partner

Stefan Ritter, Head of CERT-Bund, on the work of the Federal Administration’s Computer Emergency Response Team (CERT) of the Federal Administration in the area of tension of dynamic threat situations, about the networking of CERT-Bund and his expectations for a special CERT-Bund year 2024.

Mr Ritter, what is the current mission of the CERT-Bund team?

**Stefan Ritter:** CERT-Bund informs and warns the federal and state administrations, the operators of critical infrastructures as well as the economy and society and its national and international partners about particularly relevant and new vulnerabilities and attacks.

The field of work of all CERTs has grown considerably since the CERT was founded at the BSI in 1994. We are well positioned both internally and externally for the wide range of tasks, as we are active within national and international CERT communities. Depending on the incident, we confidently and responsibly weigh up the “need to share” against the “need to know”, i.e. at which level and in which group an overarching exchange is required. Specifically, this exchange takes place in the German CERT alliance and the administrative CERT network with the federal state CERTs. International CERT communities include the EU CSIRT network and NATO. There are also numerous trusted informal circles and bilateral contacts. Exercises such as EU Cyber Europe or the NATO Cyber Coalition further strengthen networking and exchange via collaborative platforms with functionalities for chats and indicator sharing (MiSPs).

In the area of response, CERT-Bund provides a wide range of assistance and support options. The offer ranges from specific assistance instructions, consultations with experts, selective relief and support through selected technical analyses of relevant systems to complete incident support with incident handling in a Mobile Incident Response Team (MIRT) on site and in the back office.

What does your daily work involve today, what cyber threats does CERT-Bund face?

**Ritter:** I would like to give two examples from our work. After we published the BSI Coordinated Vulnerability Disclosure (CVD) Policy last year, the number of reports to the BSI about previously unknown vulnerabilities in products within and outside the administration increased significantly. Thanks to these reports, the Warning and Information Service (WID) usually enables us to avert the threat before the vulnerabilities are actually exploited by attackers.

Since the beginning of 2023, our incident handlers and analysts have been helping those affected by attacks on the supply chain – including federal IT service providers – to analyse and deal with the incidents. CERT-Bund takes care of particularly serious incidents such as state APT attacks and – within the scope of available resources – new types of ransomware attacks that require new, complex and technically challenging solutions. We continue to see APT attacks and ransomware as the greatest threats in cyberspace. And in the future, the so-called turning point resulting from the Russian war of aggression against Ukraine and the dedicated attitude towards China will further intensify these challenges and give rise to new forms of incidents.

One particular challenge posed by supply attacks is the response and support of those indirectly affected, i.e. the customers and business partners of those affected who are directly affected by the incident. They may experience longer periods of unavailability of the purchased service or concerns about their own networks (possible lateral movement) and fear of information and data loss. This is where the crisis communication of those affected and their partners’ own security measures must work.

How does international cooperation between CERTs work?

**Ritter:** Attacks on IT and in cyberspace can take place at any time and from anywhere. The threat situation is truly unrestricted and borderless! This is precisely why national and international networks are so valuable for CERT-Bund and all other emergency response teams. The trusting and regular exchange within them is as diverse as it is helpful. Regardless of whether you need a contact person at short notice for a confidential question or a tip about a new attack vector, or whether you want to find out or check which solution approach works to eliminate a new type of attack. By exchanging information with partners, CERT professionals can share knowledge and benefit from each other. Networking and exchange are essential for this!

How can CERT-Bund keep pace with the advancing threat situation and the dynamic development of digitalisation?

**Ritter:** Our colleagues in the CERT-Bund team play a key role in this. They deal intensively with the incidents and the attack tools used every day. Thanks to their daily work and the broad-based expertise in the team, our colleagues always know what to do when there is a “fire”. In addition to this daily practice, there are of course selected training courses and participation in specialist conferences as well as the aforementioned dialogue within the CERT community. And so far, our office has given us as CERT the flexibility and freedom to use this creativity and professionalism to deal with situations and allow those affected to benefit from this. Of course, the legal framework also helps with our authorisations, which give us certainty of action.

CERT-Bund in the BSI will be 30 years old next year: What does this special anniversary mean?

**Ritter:** 30 years is a special number! The conditions under which we started back then are no longer comparable with those of today. CERT-Bund has achieved a lot in that time and is now the established professional point of contact for its target groups for the warning and information service and, above all, for emergencies. We look forward to reviewing the past years and celebrating the anniversary in 2024 with current and former companions of CERT-Bund in various formats.
NATIONAL SECURITY STRATEGY: The Federal Government will arrange for all relevant stakeholders to contribute to a comprehensive cyber situation awareness picture. The information it contains will be analysed and evaluated from a national perspective. To this end, the Federal Government will specifically improve the reconnaissance and early warning capabilities of the authorities and institutions concerned, particularly the intelligence services. The coordination function necessary for the situational awareness picture will initially be set up in the National Cyber Response Center.

MISSION STATEMENT: The National Cyber Response Center is the platform for cooperation, communication and coordination of the (security) agencies concerned, to maintain a current combined Cyber Security Situational Picture, pool strategic assessments and enable interagency incident management, by this delivering an indispensable contribution to national cyber security efforts and – in times of major crisis – to the government.

It’s Always the Single Parts That Make the Big Picture!
Artificial Intelligence

In Focus

Opportunities and Risks of Large Language Models

The Technology Has Developed Rapidly – Security Precautions Must Now Keep Pace

By Tobias Alt and Anna Wilhelm, Division Artificial Intelligence and Security

Large language models have remarkable capabilities and offer opportunities for various application scenarios. At the same time, they harbour new risks, which are grounded in the nature of the technology itself on the one hand and in the targeted exploitation by attackers on the other. A BSI publication explains the opportunities and challenges, with the most important points summarised here.

NEURAL NETWORK IN THE BACKGROUND

A large language model, or LLM for short, is a statistical model and belongs to the generative AI family. The latter is designed to learn patterns from existing data and create new data and content that also follow these patterns. Given a specific text input (so-called prompt), an LLM generates a text output that appears probable according to the model and represents the most suitable continuation of the input. The model is usually based on a neural network with billions or even trillions of parameters (hence the term large language model), which learns the probability distribution during the training process using extensive text corpora.

OppoRTUNITIES OF LLMs

In principle, LLMs can be used wherever text can be processed (partially) automatically. The possible applications range from classic editing (e. g. spelling correction) to processing (e. g. classification, creation of summaries) and generation (e. g. writing texts in a certain style). LLMs can help answer questions in chatbots, detect unwanted content such as hate speech in social networks or generate and optimise program code (e. g. to increase efficiency, correct errors, close security gaps).

RISKS OF LLMs

A first group of risks arises due to the probabilistic nature of LLMs, as they generate text based on stochastic correlations. This does not guarantee that the text is factually correct; inventing content that was not part of the input or the training data set is known as hallucinating. At the same time, the generated texts appear convincing due to their high linguistic quality, which is why unchecked use is critical. In addition, there is a lack of reproducibility and timeliness of the output and its content, possible security gaps in the generated program code and incorrect responses to prompts that significantly deviate from the training data.

The second group of risks is based on misuse. Due to their ability to generate output in different languages and mimic the writing styles of individuals or organisations, LLMs can be used to create social engineering content or misinformation. If an LLM accesses social networks, this content may be enriched with personal or company-specific information.

A third group of risks arises from attacks, e. g. in the form of so-called prompt injections. Special text inputs are used to influence the behaviour of the model so that restrictions and filter mechanisms are circumvented when processing and generating text outputs. If LLMs access external content such as websites, attackers can place instructions there that are executed as soon as the website is to be analysed. In this case, the term "indirect prompt injection" is used.

RISK ANALYSIS AND TREATMENT

In many LLMs or LLM-based applications, measures are implemented that filter out malicious input and output. These usually only partially protect against misuse and attack scenarios and offer no protection against LLM hallucinations, for example. Users must therefore be aware of the risks and conscientiously check and, if necessary, rework outputs. When using an LLM in a public authority or corporate environment, a risk analysis should be carried out for the specific application in order to detect and assess application-related risks, take appropriate measures and make a well-founded decision on the prerequisites for subsequent use.

DEVELOPMENT DYNAMICS WITH POTENTIAL

In recent years, LLMs have developed rapidly and are able to solve increasingly complex tasks with a high level of quality. This increases the potential of the models – as well as the risks associated with their use. It can be assumed that development will continue to progress rapidly and that LLMs will be increasingly integrated into systems in various application areas. This technological dynamic will therefore require an equally dynamic assessment of IT security when using large language models in the future.

Publication “Large Language Models – opportunities and risks for industry and authority”
Vulnerability report on Indirect Prompt Injections:

In Focus: Artificial Intelligence | 29
The key technology of artificial intelligence (AI) enables a wide range of digitalisation applications, such as automated driving. However, it also brings new challenges, such as a new quality and quantity of IT security risks. This article looks at the current status of the development of requirements, test methods and test tools for AI-based systems based on the automotive domain. In combination with technical guidelines from the BSI and national and international standardisation and regulatory activities, they should lead to the safe and trustworthy use of AI in the future.

The digitalisation of vehicles is making great progress. Automation not only increases comfort, for example thanks to voice control, it is also relevant for safety, as the example of lane departure warning systems shows. Many of these functions are highly complex, as they depend on highly variable sensor information, such as that which occurs on a busy road junction at different times of the day and year. Due to this complexity, direct programming usually fails. As an alternative, AI systems are used that are trained using large amounts of data. These systems are “black box” systems whose quality depends, among other things, on the quality of the training data. In addition, they can no longer be interpreted directly and cannot be formally verified. They can therefore only be tested experimentally. Last but not least, AI systems are vulnerable to adversarial and backdooring attacks, among other things.

Trust is necessary for AI systems to be accepted and used as an alternative to classical systems. For this purpose, they must be developed and implemented in a practical manner. The aim is to prove the trustworthiness of the systems.

Different aspects are tested depending on the application. When it comes to mobility, functional safety has the highest priority, i.e. the protection of health and the environment. The cyber security of AI systems in vehicles is an essential basis for road safety.

MODULAR AND USER-ORIENTATED SOLUTIONS

Due to the complexity of the task, a generalised solution approach is not initially expedient. The aim is not to develop suitable methods, criteria and tools for testing all AI systems. Instead, the BSI is pursuing a modular use case-centred approach. By working on different use cases, a modular “testing toolbox” and best practice recommendations are being developed iteratively in the various digitalisation domains. The aim is to reduce the effort required to adapt to new use cases as refinement progresses. In addition to AI and cyber security experts, expertise from the respective digitalisation domain, such as vehicle safety and IT in the mobility domain, is also required to work on the individual use cases.

With the AIMobilityAudit project, the BSI is therefore pursuing the goal of developing a modular audit toolbox for the mobility domain based on two use cases: traffic sign classification and road user recognition. The 50 audit requirements developed in the preliminary project AIMobilityAuditPrep are to be evaluated and refined. To this end, the project brings together AI, cyber security and automotive expertise from the BSI, the technology company ZF and TÜV IT. Due to the complexity of the applications and the need for empirical tests, a combination of tests will be carried out in simulations, in hardware-in-the-loop systems and on real test tracks. In order to make these tests as practical and openly communicable as possible, open source systems and proprietary industrial solutions are being evaluated in parallel. They are currently running in the laboratory and on site in Koblenz and Friedrichshafen. Among other things, specially prepared traffic signs and items of clothing are being tested to see whether – and if so, in which situations - they can mislead the classification and detection systems into making incorrect decisions.

BSI CREATES A SOLID BASIS FOR THE IMPLEMENTATION OF THE AI ACT

In the further course of the project, specific mitigation strategies will be analysed in addition to the vulnerability of the current systems. Based on the results, the creation of a modular technical guideline for testing AI systems in the automotive sector is planned for 2024. This will then serve as a template for other digitalisation domains (for example in BSI projects on the domains of medicine, agriculture and finance) and will also be used as a basis for national and international committee work in the AI and vehicle sector. The BSI thus contributes to a solid basis for the operationalisation of the European AI Act.
AI Security as a Prerequisite for Trust in Automated Driving: An Expert Discussion

What role does the cyber security of AI systems in vehicles play in the success of automated driving? Dr. Arndt von Twickel, Head of Division Cyber Security for Intelligent Transport Systems and Industry 4.0, discusses this question with Dr. Georg Schneider, Head of ZF AI-Lab Saarbrücken, and Vasilios Danos, Consultant for Cyber security at TÜV Informationstechnik, about the joint AI project AIMobilityAudit.

Dr Arndt von Twickel: Mr Schneider, you head a laboratory for artificial intelligence (AI) in the technology group ZF, which supplies systems for the mobility of cars, commercial vehicles and industrial technology. What are the key AI development projects in your area of responsibility and what kind of AI technology do you use?

Georg Schneider: We are involved in the research and application of AI in the areas of automated driving and driver assistance (AD/ADAS) as well as in process and production applications. A third area is the topic of trusted AI, which also includes the AI Mobility Audit project (see article on p. 20), which we are working on together with the BSI and TÜV Informationstechnik (TÜV IT).

We are very broadly positioned in terms of the AI technologies we use: We use both traditional methods such as decision trees and the latest deep learning technologies.

Twickel: Do you use AI technology because it is more cost-effective or because it works better than traditional software?

Schneider: Traditional and conventional algorithms very quickly reach their limits. Due to the complexity of many tasks, such as automated driving, there is often no alternative to the use of AI. When it comes to processing complex sensor information, conventional algorithms very quickly reach their limits.

Twickel: Mr Danos, what points of contact do you have with the topic of AI at TÜVIT, which specialises in the technical inspection of hardware and software? Where do you see the role of AI in mobility?

Vasilios Danos: On the one hand, we use AI as a tool for recognising complex data patterns in security analyses of smartcards, for example. On the other hand, we develop testing and certification procedures for AI systems. Our customers come from different application domains such as biometrics and mobility. We see enormous potential for AI in the mobility sector: from sensor technology and driver assistance systems to autonomous driving functions.

Twickel: From the BSI's point of view, cyber security is a prerequisite for trust in digitalisation and therefore for its success. What role does the cyber security of AI play in your work, Mr Danos?

Danos: In our view, cyber security is inextricably linked to AI and is a basic prerequisite for secure and trustworthy operation. In addition to numerous advantages, AI systems also contain a number of vulnerabilities that could be exploited by attackers. As a testing service provider, we therefore see it as our responsibility to check the security of the application.

Twickel: Mr Schneider, what role does cyber security play in the context of AI at ZF AI-Lab Saarbrücken?

Schneider: There are various departments in the ZF Group that deal exclusively with the cyber security of ZF and all ZF products. In addition to "classic" cyber security, we also want to ensure security when new types of AI attack vectors are used. This requires a deep insight into the latest AI technology in the context of the application — this is currently being analysed in the joint AIMobilityAudit project.

Twickel: What new aspects do you both see here compared to classic IT? In your view, is a new term like AI security expedient?

Schneider: I actually think this new term is necessary, as the topic has not yet been adequately addressed in an approved standard for cyber security or in any other standard. The new characteristics of AI must be taken into account. These are, for example, the "black box character" of many AI models and the huge input and parameter spaces that make so-called adversarial attacks or backdoor attacks possible.

Danos: I agree with that. A separate term could emphasise the special nature of cyber security in connection with AI and thus bundle many of the characteristics of today's AI-based applications. In contrast to classic cyber security, AI-specific vulnerabilities are not only attributable to faulty implementation or operation, but are also based on underlying machine learning processes that make it difficult to analyse vulnerabilities and investigate the causes of problems.

Twickel: In your opinion, how should AI security in mobility be tested?

Schneider: In the project, we are pursuing a use case-centred approach, i.e. we are looking at specific application examples and developing and evaluating test requirements, processes and tools. The aim here is to formulate the requirements as generally as necessary and as concretely as possible. At the same time, it is important to us that all methods and tests are designed to be practicable.

Danos: Every application has its own security requirements. Tests must therefore be risk-based and tailored to the respective application. With the growing experience from the development of test processes for various applications, common test modules and strategies can then be identified, generalised and, if necessary, automated so that the development and testing effort for new applications is minimised. We can also build on established testing processes, particularly safety and security standards in the mobility sector, and supplement these with a gap analysis with regard to AI security.

Twickel: We will probably have to wait some time for finally mature testing processes. To what extent are you already taking AI security into account in your work?

Schneider: By maintaining an ongoing dialogue with our specialist departments and our cyber security departments, we ensure that ZF incorporates the latest findings on AI security directly into the development process.

Danos: The security of AI-based applications is already a key aspect of modern vehicles. New vehicles and their (AI) components must be homologated and comply with corresponding (test) requirements in accordance with applicable standards (e.g. ISO 26262).

Twicket: What challenges do you see here now and in the future?

Schneider: A major task is embedding AI-specific tests in existing processes — new standards are needed for this in the near future. These require a joint interdisciplinary effort from industry, research and authorities. Defining test parameters and interpreting the results also remains a challenge. We have to decide what level of tolerance or residual risk we are prepared to accept.

Schneider: I agree and am optimistic that we will succeed in this task together: AI security will play an important role on the road to automated driving.

Twicket: Thank you very much for this exciting exchange!
Driver assistance systems have been increasingly used in cars for several years to enhance road safety. Since the beginning of 2020, the installation of certain driver assistance systems in new cars has even been prescribed by an EU regulation. This also includes intelligent speed assist systems. To ensure their smooth functioning, such assistants must detect the maximum speed currently permitted on the road. This is usually done using visual sensors, whose recorded data is processed by AI systems to recognise traffic signs. To ensure the smooth operation of this process, the AI systems involved have to be absolutely reliable and accurate. The AI systems must be able to recognise traffic signs correctly in all weathers and in a wide variety of situations and be robust against attacks.

ATTACKS ON NEURAL NETWORKS

The classic protection goals of IT security – integrity, confidentiality and availability – also play an important role in AI methods. AI methods can be attacked in a wide variety of ways. Typical attacks on neural networks include:

- **Adversarial attacks:** An attacker manipulates the input data in order to change the classification result of an AI system during operation. The manipulation is barely recognisable as such for humans.
- **Poisoning attacks:** This type of attack occurs during the training phase of an AI system. The attacker manipulates the training data with the aim of influencing the system’s learning process.
- **Privacy attacks:** In contrast to the previous types of attack, the focus of privacy attacks is not on manipulating the result. The aim is to obtain information about the model, about the nature of the training data or about the existence of certain data in the training set.

INTENSIVE COLLABORATION WITH STUDENTS

The BSI is investigating the impact of adversarial attacks on various traffic signalling systems. Hereby, the BSI works closely with students and supervises final theses and internships. The bachelor thesis by Steffen Jendrny from the University of Hagen focused on the use of hardware-in-the-loop (HIL) systems to evaluate the IT security of visual driver assistance systems. With HIL systems, many different cases from real driving situations can be simulated and evaluated by integrating vehicle components into a simulation. The aim of the work was to extract real attack vectors in order to draw conclusions about the vulnerability of the systems. This is a prerequisite for the creation of a methodology for the evaluation of driver assistance systems.

A SECURITY RISK AS AN INTERACTIVE EXHIBIT

The exhibit at the Deutsches Museum was developed in the context of the final thesis and interactively demonstrates how vulnerable an AI-based driver assistance system is, that automatically classifies traffic signs.

The BSI and the Deutsches Museum Bonn have been working on artificial intelligence (AI) for some time. In May 2023, the Deutsches Museum opened a new experience room on the topic of “AI in robotics and mobility”. One of the exhibits was created in cooperation with the BSI as part of a student’s thesis. The exhibit interactively demonstrates how vulnerable an AI-based driver assistance system is, that automatically classifies traffic signs.
Quantum Machine Learning Brings with It New Security Aspects

The BSI Is Investigating Threat Scenarios for Machine Learning on Quantum Computers

By Fabian Petsch, Division Artificial Intelligence – General Policy, Strategy, and Verification

The term quantum machine learning (QML) refers to a dynamic field of research that combines machine learning methods with the potential of quantum information processing. Of particular practical interest here is the extent to which certain sub-routines or even the modelling itself can be outsourced to a quantum computer in a useful way. As a competence centre for artificial intelligence (AI) in connection with IT security, the BSI is supporting the development of QML in order to work towards a secure design of the new technology.

The so-called variational quantum circuits, or VQCs for short, are currently emerging as promising methods of QML. These are characterised by an interplay between classical IT and the quantum computer: the corresponding quantum circuit typically has parameters that are adjusted iteratively using a classical optimiser. There are now a considerable number of different approaches and architectures for VQCs, including in the form of so-called quantum neural networks. Due to their comparatively low demands on the required quantum computing resources, VQCs can in principle already be realised on the currently available, i.e. not yet sufficiently error-corrected and intermediate, quantum hardware.

PARALLELS BETWEEN QML AND CLASSIC AI METHODS

When analysing the threat scenarios for QML systems and methods, it can be seen that the life cycle in a certain abstraction (data collection and preparation, model selection and training/testing, ongoing operation) is not fundamentally different from that of classic AI methods, even if the quantum components used introduce new specifics into the security assessment.

The first consideration is that the attack categories known for classic AI systems, i.e. evasion attacks, data poisoning, model stealing and privacy attacks, are at least in principle transferable to QML. In many cases, the procedures and implementations of the respective attacks, e.g. to find adversarial examples or to open a backdoor, are initially modelagnostic. Even though initial work and results already exist specifically for evasion attacks and their mitigation using adversarial training, the other attack categories are still virtually unexplored. Whether the application of the aforementioned attacks to QML is associated with a different, possibly even reduced effectiveness, has not yet been fully determined.

NEW THREAT SCENARIOS POSSIBLE

In addition to these threat scenarios motivated by the security of classic AI systems, there are also new, quantum computerspecific attack surfaces for QML. For example, the process of transpiling, in which a theoretically described quantum circuit is prepared for execution on the respective quantum hardware and adapted to its conditions, offers various possibilities for manipulation. An attacker can, for example, assign qubits with particularly high error rates and a lack of connectivity between them or even change the quantum circuit itself. A second attack vector results from the approach of executing several quantum circuits in parallel on a single quantum chip in order to effectively utilise the available resources. Unintended but physically determined couplings between the qubits (so-called cross-talk) can be utilised in this context to influence the functionality of the quantum circuit.

Even though the feasibility of such attacks has already been demonstrated, it still needs to be assessed how realistic these threat scenarios are in practice in the future.

From a scientific perspective, many fundamental relationships relating to the security of QML methods and systems, which result from the general characteristics of quantum hardware on the one hand and the specifics of QML methods on the other, have not yet been conclusively established. For example, the extent to which the attacks and defences known for conventional AI systems are influenced by the various types of noise present on the quantum computer has only been partially investigated to date. In addition, it is still unclear, for example, how different techniques for converting data into quantum states affect the resilience of QML methods.

BSI CONDUCTS BASIC RESEARCH

From the BSI’s point of view, a more in-depth examination of the security aspects of QML is strongly recommended even at this early stage. In view of the rapid progress and high investments in the field of quantum computing as a whole, the introduction of quantum computers in the application context of machine learning should be discussed with foresight. The BSI is therefore significantly involved in basic research in the form of its own project activities with regard to the attack paths, mitigation measures and other security features of QML methods and systems outlined here.
How AI Simplifies Media Regulation – Best Practice for Authorities

In addition to the projects that the BSI itself carries out or supports in the field of AI, our colleagues also regularly look outside the box and have become aware of another exciting project. The AI tool KIVI makes the work of the state media authorities easier: it makes it easier to detect depictions of violence, incitement to hatred and other offences. An interview with Ruth Meyer, Director of the Saarland State Media Authority, and Ina Goedert, Head of Media Supervision and Media Research at the Saarland State Media Authority, on the advantages of AI in the work of media supervision. The findings from working with the tool can be incorporated into future AI projects at public authorities.

What basic functions does the KIVI tool provide?
Ruth Meyer: KIVI speeds up, simplifies and improves the work of the media supervisory authority by searching the network and alerting media authority employees to possible legal violations. The way it works is the basis for the name. The name KIVI is a fusion of the terms KI and vigilare (Latin for vigilant). The focus so far has been on the protection of human dignity and the protection of minors. The specific offence categories include, for example, depictions of violence, incitement to hatred, the use of anti-constitutional symbols or freely accessible pornography. However, extensions in the area of supervisory fields that fall within the remit of the media authorities are also conceivable and have already been considered.

What was the impetus for the nationwide establishment of the tool?
Ina Goedert: The starting point was the questions of whether it is possible to react in a timely and effective manner to legal offences in a digital environment that is growing daily and whether we can find a solution that enables law enforcement on the internet across state borders in the federal system of media authorities. The answer to our questions is: Yes, we can. The KIVI tool is an aid. Every suspicion that the tool identifies is first scrutinised. The responsible organisations decide whether to initiate formal proceedings, at least on a four-eyes principle. The AI does not decide for itself! If the AI identifies a suspicion that is not confirmed, this information is also returned to the tool. Nevertheless, it is important to emphasise: The AI tool is an aid. Every suspicion that the tool identifies is first scrutinised. The responsible organisations decide whether to initiate formal proceedings, at least on a four-eyes principle. The AI does not decide for itself! If the AI identifies a suspicion that is not confirmed, this information is also returned to the tool.

How is the effect of the tool perceived by employees? And what effects can be expected in general?
Meyer: The AI learns through image and text examples that we actively feed in. These are examples that have been assessed as offences. We provide daily feedback on whether a suspicion has been confirmed or not. Therefore, the longer we work with the tool, the more efficiently the AI can learn and the better the quality of the results it delivers.

Goedert: From X (formerly Twitter) and YouTube to platforms such as Telegram and VK, the tool can automatically search more than 10,000 pages every day. Without this technical help, we could only manage a fraction of that. The significant increase in our online presence is the first major success of the tool. It enables us to find more legal offences without using our resources for the search. It also gives us an overview of the risk situation on the Internet and allows us to prioritise our pursuit of legal violations.

Our sister institution – the Media Authority of North Rhine-Westphalia (LFM NRW) – carried out a feasibility analysis in 2019 and subsequently decided to develop a tool based on artificial intelligence. Condat AG from Berlin implemented the development as a technical service provider. In 2020, LFM NRW then began developing and testing the tool so that the other media organisations could be “onboarded” from April 2022.

What are the special features of training and working with AI?
Meyer: The AI learns through image and text examples that we actively feed in. These are examples that have been assessed as offences. We provide daily feedback on whether a suspicion has been confirmed or not. Therefore, the longer we work with the tool, the more efficiently the AI can learn and the better the quality of the results it delivers.

Nevertheless, it is important to emphasise: The AI tool is an aid. Every suspicion that the tool identifies is first scrutinised. The responsible organisations decide whether to initiate formal proceedings, at least on a four-eyes principle. The AI does not decide for itself! If the AI identifies a suspicion that is not confirmed, this information is also returned to the tool.

How is the effect of the tool perceived by employees? And what effects can be expected in general?
Meyer: The AI learns through image and text examples that we actively feed in. These are examples that have been assessed as offences. We provide daily feedback on whether a suspicion has been confirmed or not. Therefore, the longer we work with the tool, the more efficiently the AI can learn and the better the quality of the results it delivers.

Goedert: From X (formerly Twitter) and YouTube to platforms such as Telegram and VK, the tool can automatically search more than 10,000 pages every day. Without this technical help, we could only manage a fraction of that. The significant increase in our online presence is the first major success of the tool. It enables us to find more legal offences without using our resources for the search. It also gives us an overview of the risk situation on the Internet and allows us to prioritise our pursuit of legal violations.

How can interested parties find out more about the topic or even help?
Goedert: We take a very transparent approach to the use of AI and are grateful for any information on improving our methods and AI systems. Among other things, we rely on keyword and link-based searches for content on the open Internet and on social platforms such as scraping or link extraction. Images and texts are analysed with AI methods using neural networks and pretrained models and services (Convolutional Neural Network, Transfer Learning, Amazon Recognition Unsafe Content) and classic statistical machine learning methods (Naive Bayes method). Any suggestions for improvement and possible data gaps are therefore welcome from all media organisations.
Building the Cybernation
Germany Together

Only with Hard Work, We Can Increase Cyber Resilience Substantially.

An Interview with Claudia Plattner, BSI President

Dear Claudia, how have you settled in to your new role as Germany’s top cyber security chief? What was your impression?

Nice job title, but I do not see myself as someone like that. In the initial period, my focus was gaining a comprehensive overview. All the cyber security experts – all my colleagues at the BSI – have been wonderfully helpful. After all, they are the guarantors that we are „up and running“. After many introductory meetings and intensive exchanges, I have experienced a steep learning curve, but I am far from finished with learning. I felt warmly welcomed and found the insights fascinating, and the discussions were fruitful. I still feel that way.

My impression after the first 100 days: We are in an enormous field of tension.

A wide variety of factors are affecting us in a complex situation, ranging from geopolitical tensions to an increasing threat situation in cyberspace and a generally tense atmosphere in society, with people fearing that Germany is missing digitalisation. Taking the helm in this situation is a major task that I am happy to take on. If we position ourselves well, prepare ourselves well and, above all, cooperate well, we can do it.

Keyword threat situation: How do you assess the state of IT security in Germany?

The report on the state of IT security in Germany, which we presented at the Federal Press Conference in early November 2023, paints a worrying picture. We have a serious problem: a quarter of a million new malware variants and 21,000 infected systems every day, along with more than 2,000 vulnerabilities in software products per month. According to the digital association bitkom, the damage caused by attacks on German companies amounts to over 200 billion euros. This constitutes 43 per cent of the entire federal budget, to put the figure into perspective.

What do you think are the most serious reasons for this situation?

There are many threat scenarios. I would like to highlight five points that are interlinked:

Cyber attacks with ransomware are still the most pressing problem. Beside the associated high costs and the lasting disruption to value chains, I see the diminishing trust in the state, administration and ultimately in digitalisation as critical. On average, two municipalities and municipal companies are affected every month.

Often, the data is not only encrypted but also stolen, with a threat of publication. This we call double extortion. This data theft poses another problem: espionage. Disclosing business secrets or confidential information can lead to competitive disadvantages. If it is not just about commercial details, we are talking about political motivation, which, considering the geopolitical situation and hybrid threats, leads us to sabotage.

In the worst-case scenario, attackers can disable critical infrastructure. What we see on a daily basis – and their intensity and danger is increasing – are DDoS attacks that also disrupt the activities of governmental organisations.
We must prioritise cybersecurity. Only when decision-makers at the highest level recognise the importance of the issue fundamental improvements take place. We must increase cyber resilience substantially. This requires a significant amount of hard work.

We must promote digitalisation in a sustainable way. Modern technologies are more easily protectable. When all systems are up to date, we can leverage security advantages. We must develop and research key technologies. This includes AI, quantum, eID and cloud solutions.

We must consolidate our technological expertise. To harness the full technological potential of cyber security, we need coordinated cooperation between all players and across all borders.

Even though these attacks are primarily used for propaganda purposes, this point leads to the next scenario: Political influence through disinformation. Deepfakes on social media platforms are used to influence opinions, manipulate elections or even destabilise societies.

What is particularly alarming in all these threat scenarios is the increasing professionalism, the use of state-of-the-art technology such as AI and the division of labour, especially in ransomware attacks. „Cybercrime-as-a-service“ is on the rise.

How can we gain control of this situation?

Even simple measures can significantly increase information security: install updates regularly, use secure passwords, disable macros, create regular data backups in a way that malware cannot encrypt them and regularly prepare for emergencies. We consistently advise this, especially to small and medium sized companies.

We also offer cities and local authorities a low-threshold medium sized companies. We consistently advise this, especially to small and regular updates with simple test questions and accompanying tools, local authorities can identify and implement the most urgent measures themselves. This allows for an initial but essential step towards systematic information security.

The IT security label is another example: it provides transparency for consumers in areas such as smart home multimedia. Products with our label meet basic security standards, providing guidance for informed purchasing decisions and promoting protection against cyber-crime. We are thus incentivising the consumer market that information security is an important factor when purchasing and using IT products.

Is that enough in your opinion?

No, by far, that is not enough. The topic of cybersecurity requires thinking on a grand scale. Germany must see itself as a cyber nation. We – all of us as a community – must express this self-perception and follow up with actions.

The topic of cybersecurity requires thinking on a grand scale. Germany must see itself as a cyber nation.

We must actively shape cybersecurity. Rapid clarity about the security features of tomorrow’s products creates certainty of action. Our specifications and requirements for certification and standardisation already address this issue. Our standards in IT baseline protection or our technical guidelines are available as specifications and working tools that help authorities, companies and institutions to help themselves.

We must create a cyber market. In a thriving cyber ecosystem involving the triad of politics, science and business, secure digital products can be researched, developed, and then actually used to increase cyber security.

Who do you need as partners to implement this vision?

Everyone. Each and every one! Building the cyber nation Germany together.

We must proactively protect ourselves better against cyber attacks and practice emergency response. It is no longer a question of if but when we will be affected. We need to be capable of helping each other and quickly restoring normal operations.

In the end, that is the ultimate goal, because there is no such thing as one hundred per cent security. We, as enablers, partners and helpers work on this every day. Let us tackle it together!
The security of 5G networks is of great importance, as they form the foundation for many applications and services that impact our daily lives. Testing of the 5G systems requires considerable effort and has to take into account many special cases, due to the high complexity of the 5G standard.

BSI aims to make relevant contributions to IT security in the context of mobile network infrastructures. This necessitates work within its own 5G/6G Security Lab, which is why TEMIS was planned and established.

The Security Laboratory “Test Environment for Mobile Infrastructure Security” (TEMIS) to contribute to the continuous improvement of mobile network security in Germany. TEMIS provides, in addition to 5G networks (and later 6G networks) from various manufacturers, corresponding measurement and testing equipment with a focus on security-related tests.

For the BSI is cyber security in mobile infrastructures. With the first development stage of the 5G/6G Security Lab at the BSI site in Freital, we have achieved an important milestone. BSI aims to continuously enhance the security level and resilience of national and private 5G networks. The 5G/6G Security Lab, for example, is used to update requirements and guidelines for network operators practice-oriented in accordance with the Federal Network Agency. Other key areas of focus include certification, standardisation, and security tests.

DEVELOPMENT AND VALIDATION OF CERTIFICATION TESTS

The IT-Security Act 2.0 rendered the certification of critical 5G network components legally mandatory in Germany. For 5G equipment, BSI primarily develops the NESAS CCS-GI scheme (Network Equipment Security Assurance Scheme Cybersecurity Certification Scheme – German Implementation). NESAS uses the Security Assurance Specifications (SCAS) defined by the 3GPP – the standardisation body for 5G – as test requirements. BSI has the task of defining and specifying the testing foundations for evaluation bodies. To achieve this, SCAS tests must be validated, specified, and potentially expanded. These additions are evaluated in TEMIS. Test instructions and interpretations are technically verified and subsequently published in the document “Application Notes and Interpretations for the Scheme” (ANS-N2). TEMIS also serves to replicate and assess issues reported by evaluation bodies during the execution of test cases. To facilitate the reproducibility and automation of test cases, the TEMIS team at BSI additionally develops its own test software tool: the SCAS Test Framework.

SHAPING SECURE STANDARDS

The principle of “Security by Design” must already be considered during the development of standards and test specifications for 5G mobile networks. Therefore, BSI engages in 3GPP standardisation groups to actively shape, improve, and if necessary initiate new SCAS tests. The necessary knowledge is primarily gained through hands-on work with 5G technology and related security products. TEMIS allows the technical implementation of customised test case designs as well as the validation of existing tests or those proposed by third parties. The contributions resulting from the BSI’s work in standardisation committees strengthen IT security. Simultaneously, BSI integrates the experiences gained in Germany into the work of EU committees for a European 5G certification scheme.

COLLABORATION WITH RESEARCH AND DEVELOPMENT

BSI has initiated numerous 5G/6G security projects in the scope of its own funding programme. The spectrum of funded project members ranges from 5G evaluation bodies to larger research consortia and start-ups. These projects, as well as security researchers, can validate their results using the 5G/6G Security Lab test capabilities. Initial analyses with scientists have already been conducted successfully.

The BSI team is now looking forward to using intensively the new IT security capabilities made possible by TEMIS.

Further information from the BSI on 5G:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/5-G.html

Further information on BSI’s funding programme (KoPa45):

https://www.bsi.bund.de/dok/KoPa45
Ransomware, Vulnerabilities and Resilience

Once a year, the Federal Office for Information Security reports on the state of IT security in Germany. In this year’s report, the BSI concludes that the threat level is higher than ever before. The professionalisation of attackers in cyberspace continues unabated. The state, economy and society need appropriate defences.

RANSOMWARE REMAINS THE BIGGEST THREAT
The BSI is observing a shift in cyber attacks using ransomware. The focus is no longer on large, financially strong companies, but increasingly also on small and medium-sized organisations as well as state institutions and local authorities. The citizens of our country are often directly affected by successful cyberattacks on local authorities and municipal organisations as well as state institutions and local authorities.

SOFTWARE VULNERABILITIES AT AN ALARMING LEVEL
The BSI is recording more and more software vulnerabilities. These vulnerabilities are often the gateway for cyber criminals on their way to compromising systems and IT networks. With an average of almost 70 new vulnerabilities in software products per day, the BSI has not only recorded around a quarter more than in the previous reporting period. As the number increased, so did their potentially damaging effect: more and more vulnerabilities (around one in six) are being classified as critical.

ON THE RISE: CYBERCRIME-AS-A-SERVICE
Like the real economy, cybercriminals are increasingly relying on the division of labour, a growing range of services and close networking across national and industry boundaries. With the concept of “cybercrime-as-a-service”, cybercriminals are acting more and more professionally, as specialising in certain services enables them to develop and use their “services” in a targeted manner.

EFFECTS OF THE WAR IN UKRAINE ON THE IT SECURITY SITUATION IN GERMANY
The Russian war of aggression against Ukraine continued to take centre stage in public perception during the reporting period. However, DDoS attacks by pro-Russian attackers registered by the BSI have so far caused little to no lasting damage in Germany. The BSI categorises the attacks to date more as propaganda. They are intended to create uncertainty and undermine trust in the state. However, this strategy can also change, as the past has shown.

GENERATIVE AI CREATES NEW RISKS, BUT ALSO NEW OPPORTUNITIES
With ChatGPT, Bard and LiaMa, as well as a number of other tools, artificial intelligence has reached a broad, even less tech-savvy public. These tools are easy to use and deliver high quality output. However, they can also be misused for criminal purposes. For example, they can ensure that so-called deepfakes – manipulated images, videos and voices – become more and more authentic, making them increasingly difficult to unmask. AI can also make phishing emails more credible, and more authentic, making them increasingly difficult to support the “services” of a targeted manner.

A new trend can rarely be stopped. In a potentially critical situation such as the Russian war of aggression against Ukraine, it is crucial to weigh up whether this method will bring financial gain for the attackers. If attacks become easier or the chance of success for an attack increases, there is a risk that the method will spread and quickly become a new trend.

GROWING RESILIENCE AGAINST INCREASING THREATS
In a comprehensively networked society there can be no one hundred per cent security against attacks on IT infrastructures and software-controlled devices. However, the best protection against such attacks is a high level of cyber resilience. This involves increasing the resilience of IT and being able to counter attacks better.

More qualified security experts are needed to make IT systems more resilient, ward off attacks and, in the event of a successful attack, minimise the negative consequences. Here, professionalisation on the defence side helps – among other things – through standardisation, centralisation and automation. The state and civil society are not defenceless in the face of the diverse threats in cyberspace, but can certainly counter them successfully. The BSI, as the federal cyber security authority, is there to support them.

Alexander Härtel, National IT Situation Centre, Analyses and Forecasts

INSIGHT INTO THE CYBER SECURITY ENGINE ROOM – WHEN AN INCIDENT BECOMES A TREND
The BSI records trends in the threat situation with its threat intelligence team. This team observes attackers and their behaviour over a longer period of time. This allows the BSI to categorise reports and incidents in a wider context and recognise trends. In addition, technical indicators are also obtained which are used to actively protect computer systems, e.g. within the federal administration.

Every trend described in the BSI Situation Report 2023 started out small. For example, a single attacker group develops a new method such as blackmailing with a leak page on the darknet. This new method can become known to the BSI in various ways. An affected person can contact the BSI’s National IT Situation Centre. Both nationally and internationally, the BSI is in constant dialogue with IT security analysts, partner authorities and CERTs. In addition, the BSI also purchases threat intelligence from commercial providers in order to track threat developments outside of Germany, as attackers rarely stop at national borders. And that is just the tip of the iceberg.

As soon as a new method becomes known, various questions arise. In the case of financially motivated attackers, it is crucial to weigh up whether this method will bring financial gain for the attackers. If attacks become easier or the chance of success for an attack increases, there is a risk that the method will spread and quickly become a new trend.

As almost every component of an attack is now offered as a service, a new method quickly becomes available to many attackers. A dynamic can also be observed between cyber criminals who offer these services. Methods are adopted, developed further and made available to even more attackers. Within a few months, ransomware extortion has become double extortion – blackmailing the victim by encrypting their data and simultaneously threatening to publish the stolen data.

As soon as a new trend becomes known, various questions arise. In the case of financially motivated attackers, it is crucial to weigh up whether this method will bring financial gain for the attackers. If attacks become easier or the chance of success for an attack increases, there is a risk that the method will spread and quickly become a new trend.

The Russian war of aggression against Ukraine continued to take centre stage in public perception during the reporting period. However, DDoS attacks by pro-Russian attackers registered by the BSI have so far caused little to no lasting damage in Germany. The BSI categorises the attacks to date more as propaganda. They are intended to create uncertainty and undermine trust in the state. However, this strategy can also change, as the past has shown.
The State of IT Security in Germany in 2023

Ransomware remains the biggest threat.

2 Ransomware attacks on local governments or municipal businesses were reported on average per month.

68 successful ransomware attacks on companies became known.

15 of them were directed against IT service providers.

2,000 more than vulnerabilities in software products (15% of which were critical) became known on average per month during the reporting period. This is an increase of 24%.

A quarter of a million new malware variants were found on average every day during the reporting period.

66% of all spam in the reporting period were cyber attacks: 34% extortion mails 32% fraud emails

84% of all fraudulent emails were phishing emails to obtain authentication data, mostly from banks and savings banks.

Top 3 Threats per Target Group

Civil Society
Identity theft
Ransomware

Industry
Ransomware
Dependency within the IT supply chain, Vulnerabilities, open or incorrectly configured online servers

State and Administration
Ransomware
API, Vulnerabilities, open or misconfigured online servers

Around 21,000 infected systems were detected daily in the reporting period and reported by the BSI to the German Providers.

On average, around 775 emails with malware were detected daily in the reporting period and reported by the BSI to the German providers.

370 websites were blocked from access from government networks on average each day of the reporting period. The reason: the websites contained malware.

6,220 participants had joined the Alliance for Cyber Security by 2023.
Cyber Security on the Agenda:
The BSI at it-sa Expo&Congress

At this year’s it-sa Expo&Congress, which took place from 10 to 12 October 2023 in Nuremberg, various topics were on the BSI’s trade fair agenda to build the cyber nation Germany. Numerous BSI employees presented their solutions, products or project results at the highly frequented BSI stand and exchanged ideas with visitors on a professional level. Three colleagues provide an insight into their days at the fair.

MICHAEL KRAUSS, CYBER SECURITY FOR SMALL AND MEDIUM-SIZED ENTERPRISES DEPARTMENT

“The protection of small and medium-sized enterprises is very important to my team colleagues and me. At our presentation stand, supported by our information materials, we were able to inform interested stand visitors about measures to increase their cyber security in a large number of discussions. We pointed out to IT service providers how they can securely accompany small and micro-enterprises into the digital future using DIN Spec 27076 “IT security consulting for small and micro-enterprises”, which we helped to develop. In the Speakers Corner, my head of department Manuel Bach provided information on the dangers of using information technology and gave advice on how companies can better position themselves. It is not that difficult to protect yourself. The BSI offers a range of services in this area.

The trade fair was once again a well-rounded event and, from my personal point of view, a complete success. We’re looking forward to the next one: it-sa 2024 in Nuremberg; here we come!”

MARION DEMAND, VIRTUALISATION AND CLOUD SECURITY DEPARTMENT

“I represented the cloud team of the BSI with my colleague Heiko Großkopf at it-sa. We were mainly asked basic questions about secure cloud usage, cloud migration and the CS. It was important for us to emphasise a very well thought usage of the technology and to take note of the shared responsibility between service provider and customer to secure cloud services. Furthermore we discussed some specialised topics such as edge computing and digital sovereignty with some visitors to the fair. In addition to the stand service, I presented aspects of a secure cloud usage in a short talk in the Speakers Corner of the BSI.

Taking part in it-sa was very enriching, especially getting to know the special use cases and perspectives from the field. But the dialogue with colleagues at the stand was also very inspiring. My conclusion: although the stand work was exhausting, the positives outweighed the negatives. I’m already looking forward to my next assignment at it-sa.”

DANIEL GILLES, BSI STANDARDS AND IT-GRUNDSCHUTZ DEPARTMENT

“For me, it-sa is always an excellent opportunity to get in direct contact with our users. This allows me to pick up on current trends for our team and discuss the latest developments in IT Baseline protection in personal conversations. A key topic this year was the various levers for optimising IT-Grundschutz, such as the reduction of documentation costs or the integration and synergy with other topics such as BCM, minimum standards, etc.

My personal concern is that we involve our various target groups in these topics at an early stage and that we engage in open discussion. It-sa is the opportunity to do this.”
Improving Germany’s IT Security


By Marc Brauer, Martin Kurtz and Rhian Moritz, Division IT Security and Law

The BSI works to recognise and eliminate attacks as well as gaps in the IT security of the federal administration. The authorisations and processes in the cooperation between the Federal Office and other institutions are precisely regulated. The BSI acts both in the background and preventively as well as operationally, even on site in exceptional cases.

The BSI operates several systems for the federal administration to detect and defend against malware. These include, for example, a malware detection system, a malware prevention system and the federal cloud service Detection-as-a-Service. The BSI may use these programmes to analyse log data, logging data and so-called interface data both automatically and manually in accordance with Sections 5 and 5a BSIG to prevent threats to the federal government’s communications technology.

The BSI has the task of recognising and eliminating attacks as well as gaps in the IT security of the federal administration. The authorisations and processes in the cooperation between the Federal Office and other institutions are precisely regulated. The BSI acts both in the background and preventively as well as operationally, even on site in exceptional cases.

The BSI works to recognise and eliminate attacks as well as gaps in the IT security of the federal administration. The authorisations and processes in the cooperation between the Federal Office and other institutions are precisely regulated. The BSI acts both in the background and preventively as well as operationally, even on site in exceptional cases.

SCANNING AUTHORISATION – WITH RESTRICTIONS

“The BSI is becoming a hacker authority!” Most colleagues can certainly remember this striking headline. The reason for this media coverage was the so-called scanning authorisations contained in Section 7b BSIG. This authorisation enables the detection of security vulnerabilities and other security risks at the interfaces between the telecommunications network and the federal administration as well as KRITIS, UBiS and digital services in accordance with Section 2 (11) BSIG.

The scans may only be carried out using the “white list”, which contains the IP addresses of the abovementioned bodies and organisations. However, an actual scan may only be carried out on unprotected systems. A system is unprotected if there are publicly known security vulnerabilities or other obviously inadequate security precautions.

If the BSI recognises a security vulnerability or inadequate security precautions by means of a scan, it must inform those affected immediately. If possible, specific information on how to remedy the situation must be provided. The BfDI is informed annually by the BSI about the scanning measures carried out in accordance with Section 7b BSIG.

DEPLOYMENT OF A MOBILE INCIDENT RESPONSE TEAM

The deployment of a Mobile Incident Response Team (MIRT) can certainly be considered the most striking headline. The reason for this media coverage was the so-called scanning authorisations contained in Section 7b BSIG. This authorisation enables the detection of security vulnerabilities and other security risks at the interfaces between the telecommunications network and the federal administration as well as KRITIS, UBiS and digital services in accordance with Section 2 (11) BSIG.

The scans may only be carried out using the “white list”, which contains the IP addresses of the abovementioned bodies and organisations. However, an actual scan may only be carried out on unprotected systems. A system is unprotected if there are publicly known security vulnerabilities or other obviously inadequate security precautions.

If the BSI recognises a security vulnerability or inadequate security precautions by means of a scan, it must inform those affected immediately. If possible, specific information on how to remedy the situation must be provided. The BfDI is informed annually by the BSI about the scanning measures carried out in accordance with Section 7b BSIG.

CONCLUSION

The overview of the BSI’s powers vis-à-vis the federal administration shows that the BSI fulfills a wide range of tasks in very different areas. However, the aim of all its actions and recommendations is to increase Germany’s IT security.

To achieve this, all three of the BSI’s areas of activity (security guidelines and checks, information activities and operational activities) are equally important. Even if operational activities have a greater impact, especially externally: If, for example, a federal server has been attacked and a MIRT is deployed that can reverse its functions, this is of course particularly tangible. However, the collection and evaluation of information and the effectiveness of standardisation powers are equally important tools in the BSI’s daily work against cyber threats and for greater IT security.
Personnel Development at BSI Promotes Professional Competences as well as Leadership Skills and Team Spirit

By Anna Eichhorst, Anke Gaul, René Karle and Mareike Mumm, Division Human Resources Development #TeamBSI

The future is uncertain, but not predetermined. Anyone who is part of #TeamBSI can help shape this future, which is what makes the work so exciting. In addition to a high level of expertise, this also requires a growth and development-oriented mindset, which is crucial for how problems, challenges and tasks are dealt with. BSI’s HR development measures are consistently geared towards both – in individual training, in management development, and with an outlook towards optimising collaboration and cooperation.

In a dynamic cyber environment, keeping an eye on the future means being ahead of the game. This applies not only to technological progress, which brings new applications as well as new attack scenarios, but also to the people in #TeamBSI who face these challenges.

Knowledge in the IT sector has an extremely short lifespan and is subject to continuous change. The demands met by the specialists from #TeamBSI who use their expertise to protect the BSI and thus IT security as a cornerstone of society are therefore high.

At the same time, we achieve the best results as a team. With regards to the future, the BSI has therefore been investing heavily in modern personnel development for years. An environment of continuous learning is not a nice-to-have, but an attractive employer on the labour market.

For leadership to be successful, i.e. to have a positive effect on the overall performance of the organisation, it requires acceptance of one’s own role as a manager, for which many more competencies are decisive than “just” the technical ability to assess a topic.

In order to make these requirements more transparent and tangible, the BSI has described the key skills and abilities that people in management positions should have and constantly develop competence model for managers at the BSI. The model is continuously adapted and serves as a valuable basis and effective tool for the targeted personnel development of our managers and junior managers as well as for recruiting at these levels.

Another strategic management element is the Leadership@BSI_2025 process initiated in 2019: getting to know innovative management tools, taking up current leadership impulses in short workshops and lectures, intensifying dialogue in new formats, but also developing the next generation of managers from within our own ranks are exemplary measures that complement the classic range of training and support, for example through coaching.

**FOCUS ON FUTURE SKILLS**

But it is not only the demands on managers that are changing. The world of work requires all employees to adapt quickly, for example towards lifelong learning, the digitalisation of work equipment and collaboration, and the new complexity of information. At the same time, employees in #TeamBSI can help shape the future. To this end, we have supplemented the competency model with so-called future competencies, which were jointly developed and adopted in HR development with stakeholders and future shapers. In addition to specific competences, a general growth and improvement-oriented attitude is crucial.
Future Profession: Digitalization and Cyber Security?

Take on exciting tasks and provide a valuable contribution to secure digitalization in Germany. There are various opportunities to join the #TeamBSI.

INTERNSHIP
Are you looking for a compulsory or voluntary internship (minimum 10 weeks) and want to take on exciting tasks in the field of cyber security?

FINAL THESIS
No topic for your Bachelor’s or Master’s thesis yet and interested in topics such as cloud security, AI, digital consumer protection or automotive?

DIRECT ENTRY
Take a look at our careers page – there you will find numerous exciting vacancies on a wide range of cyber security topics. If you can’t find anything suitable, please send us an unsolicited application via our “digital talent” announcement and become part of the #TeamBSI, too.

Further information on www.team-bsi.de
The WiBA Project: An Easy Introduction to Cyber Security for Municipalities

First Steps into IT-Grundschutz Basic Protection Using Simple Means

By Carmen Gros and Florian Hillebrand, WiBA Project Group

The new “Pathway to Basic Protection” (WiBA) offers a low-threshold introduction to BSI’s IT-Grundschutz for small municipalities, in particular free of charge. Using checklists with simple questions and corresponding additional resources, local authorities can now identify and implement the most urgent safeguards themselves. This enables them to take a first but essential step towards systematic information security.

In recent years, there have been several successful cyber-attacks on local authorities - some with serious consequences and a great deal of media coverage. For cyber criminals, local authorities are an enticing target with great potential for damage. Such attacks are often facilitated by only rudimentary protection, in many cases because only limited resources for information security are available.

Standardised methodologies for setting up an information security management system (ISMS) to enable the systematic implementation of security safeguards are often very complex. Although for example BSI’s IT-Grundschutz offers a simplified entry-level methodology with the so-called Basic Protection, even this is often perceived as too complex by the municipal sector.

In autumn 2022, BSI therefore initiated the “Pathway to Basic Protection” (WiBA) project to simplify starting with information security and make it more practical, especially for local authorities.

Using checklists for specific topics and in close consultation with local authority stakeholders, an approach was created to determine the status of information security and to identify essential actions for improvement, even without in-depth knowledge of a formal methodology.

The checklists cover fundamental security requirements for about 20 relevant areas of information security. This includes checklists for technical topics such as server systems or backups, but also checklists for organisational areas, such as preparation for IT security incidents.

With the new entry level, local authorities can build up a level of protection that they can seamlessly raise to the level of the IT-Grundschutz profile “Basic Protection for Local Authorities”.

THE CHECKLIST CONCEPT

Based on the IT-Grundschutz profile “Basic Protection for Local Authorities” which is created and maintained by the “Working Group on Basic Protection for Local Authorities” (AG Koka), the WiBA project identified the key topics and essential requirements for information security that are relevant in the local authority environment.

The requirements were then translated into checklist questions that enable the responsible parties in local authorities to survey the current status of information security by using simple yes/no questions.

Many of the checklist questions also contain additional resources that support the implementation of respective safeguards. These resources usually consist of specific explanations but can also contain references to further information provided e.g. by BSI.

SUCCESSFUL FIELD TRIALS IN MODEL MUNICIPALITIES

In order to make the checklists as practical as possible, a pilot phase with model municipalities was already planned at an early stage of the project. In response to a corresponding call in February 2023, BSI received over 130 applications from interested municipalities. Six model municipalities were selected based on various criteria such as size, regional location and previous experience in the area of information security. A workshop lasting several days took place in each of these municipalities in May and June 2023 to gather practical experience and feedback. The feedback on WiBA was very positive and could already be incorporated into the checklists before publishing them as publicly available community drafts in August 2023.

PUBLICATION AND NEXT STEPS

The community drafts also received comprehensive and very positive feedback, which shows the importance of a simple entry-level introduction to information security and the great demand for it.

The checklists were revised again on this basis and published in time for the it-sa IT security expo and congress in Nuremberg in October 2023.

However, WiBA is a “living” project: not only will the additional resources be continuously expanded in order to make the checklists even more helpful and practical. WiBA must also adapt as soon as the IT-Grundschutz profile “Basic Protection for Local Authorities”, on which the checklists are based, is updated.

Further information:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basic_Absicherung_Kommunale_zuweisung.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Basis_Absicherung_Kommunale_zuweisung.html
Making Cyber Security More User-Friendly

The Directorate-General BL at the BSI Develops User-Friendly Security Concepts for Federal, State and Local Authorities

By Philipp Deuster, Division Minimum Standards for the Federal Administration, Claudia Gola, Division IT Security Consulting (Saxony Section), and Moritz Lechleuthner, Directorate-General Consulting for Federal, State and Local Governments

Usability in cyber security has been the focus of governmental attention at least since the Cyber Security Strategy for Germany 2021. Albeit always having been a part of BSI’s security approach, only in recent years has it been identified as one of the key factors of driving successful cyber security implementation. The reasoning is as clear as it is simple. Even the most secure solution or the best concept can increase security only if users actually use it. The Consultancy Department for Federal, State and Local Authorities (BL) is therefore increasingly developing user-friendly prevention requirements and specifications for public bodies.

The BSI has been working on usability in cyber security for years. At the centre of its preventive measures lies its own IT-Grundschutz methodology, a systematic approach that is compatible to, but also more comprehensive than, the ISO/IEC 27001 standard. Concerning federal government agencies, a recent report on the now completed project “Repositioning IT-Grundschutz for the federal administration” (NIT-GSB) by the BL 13 unit Information Security Consultancy Saxony received a great deal of feedback. As NIT-GSB also focused on promoting better usability of bespoke IT-Grundschutz for federal government agencies, numerous responses highlighted a desire for even more support and, simply, easier application. BL 13 responded by selecting key points from the NIT-GSB project for working out usability measures that meet users’ requests. To better manage follow-up activities, BL 13 founded the “Coordination body for the federal administration to strengthen IT baseline protection” – KoBIG for short.

Some of these measures include the development of a collaboration platform for information security officers (ISOs), creating and providing user-friendly work aids in the form of an online toolbox, and the development of additional IT Grundschutz profiles. Furthermore, the automation possibilities of the federal government’s information security management system (ISMS) are projected to hold great potential for significantly reducing administration work and are therefore being looked into by KoBIG as well.

CUSTOMISED ASSISTANCE FOR FEDERAL AGENCIES

One of the most important tools for usable cyber security in federal government is the Federal Minimum Standards framework, which the BSI’s BL 35 unit of the same name has been coordinating in collaboration with the IT-Grundschutz unit SZ 13 and the BSI’s technical units since 2014. Minimum requirements are drawn up for specific use cases in the federal government, taking into account its specific, and sometimes unique, conditions. The federal agencies thus receive specifications and customised assistance based on IT-Grundschutz in order to implement cyber security requirements in practice. Extensive external and internal BSI coordination processes ensure that already published regulations are taken into account and are referenced where necessary. Additionally, references to IT-Grundschutz are made available in an editable format that users can use to integrate the requirements into their toolboxes. In the future, the NIS 2 Implementation Act will also make the application of IT-Grundschutz mandatory in the federal administration at large. As the Minimum Standards framework already takes into account IT-Grundschutz and offers practical assistance for specific applications, federal agencies should be able to adapt quickly and sustainably. At the same time, the BSI is working on harmonising the Minimum Standards framework and IT-Grundschutz approach even further, so as to make implementation easier and thus the federal government more secure.

COMPLEX DIGITALISATION REQUIRES COMPLEX SECURITY SYSTEMS

These selected examples show how, not only the BL department but the entire BSI increasingly incorporates usability into cyber security. The complexity of increasing digitalisation in more and more areas of work and life naturally applies to its security as well. As the competence centre for cyber security in Germany, it is BSI’s mission to provide users with increasing support to easily and effectively implement cyber security measures and to improve the necessary conditions for this by taking usability into account. As such, the examples above are just an excerpt. While the BL 12 and SZ 13 project “Wege in die Basis-Absicherung” (Paths to Basic Protection) supports local authorities in getting started with IT-Grundschutz (see article on p. 48), the BSI’s plan to harmonise confidentiality requirements and cyber security requirements will be the subject of an upcoming BSI magazine article.
Usable Security as a Quality Feature of IT

BSI Project Develops Principles and Guidelines for User-Friendly IT Security from a Consumer Perspective

By Dr. Matthias Korn and Kristina Unverricht, Division Basic Issues of Digital Consumer Protection and Cooperations, and Prof. Dr. Therese Mieth, Federal University of Applied Sciences for Public Administration

In a joint project with the Federal University of Applied Sciences for Public Administration, the BSI is focusing on the topic of usable security from a consumer perspective. The aim is to provide support for the implementation of usable security in the design of information technologies. The focus is on usability, accessibility, transparency and acceptance. These four areas are critical success factors in order to implement IT security in the practical everyday use of information technologies.

GUIDELINES FOR DEVELOPERS

In the project with the Federal University of Applied Sciences, the success factors for usable security are being compiled and guidelines that support developers in the user-friendly design of security technologies in products and services will be developed. In future, these guidelines may also feed into the design of standards and specifications, as well as into regulatory processes. Criteria for usable security may also be taken into account as success criteria in public procurement processes.

For users, IT security is generally not an objective in itself. They usually have other needs and goals. Security mechanisms must therefore be designed in such a way that they are easy to implement and can be integrated into the user's everyday life and routines. In this way, a high level of practical IT security can be guaranteed. This is the goal of usable security.

Usable security is to be understood as a quality feature of IT security that leads to greater acceptance among users of digital technologies through usability, accessibility, transparency and a positive user experience. This in turn increases IT security in actual use.

Building on current research findings in the field of usable security, the project takes a broad approach and considers the four areas of usability, accessibility, transparency and acceptance.

GUIDELINES FOR DEVELOPERS

The first result of the project is a systematic overview for the BSI, which identifies the most important issues for usable security. To this end, relevant research results as well as standards and specifications in the field of usable security were analysed. The systematic overview is primarily aimed at IT security experts in order to help them address usable security requirements. In the next step, the model will be reviewed and refined using sample projects in order to promote the development of user-friendly and secure technologies in the long term. Usability and IT security are not in contrast to each other, but belong together. This is because an increase in user-friendly design leads to increased IT security.
Advantages of “Infrastructure as Code” in the Cloud

The Provision, Configuration, Update and Deletion of Cloud Services by Code

By Jan Bings, Division Virtualization and Cloud Security

“Infrastructure as Code” (IaC) significantly simplifies the application of security requirements: scripts created using IaC can provide and manage everything from individual virtual servers to complex application scenarios. In this way, IaC can support authorities and companies in the secure use of the cloud.

“Infrastructure as code” (IaC) describes a concept that enables the provision and configuration of resources based on scripts or code. Using IaC, cloud services ranging from Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) to Software-as-a-Service (SaaS) can be provided, configured, updated and deleted. IaC is not a new concept and is also established in on-premises infrastructures. One difference is that the number of possible resources tends to be higher with most cloud providers, as cloud platforms usually provide virtualised resources and customers do not have to create scripts to implement IaC themselves. The scripts are based on standardised formats such as JavaScript Object Notation (JSON) and YAML Ain’t Markup Language (YAML) and are transmitted to the defined API services of the cloud providers. The code is provider-specific and there are different mandatory parameters, meaning that the scripts have to be adjusted before being transferred to other providers.

opportunities through IaC

One advantage of deploying and updating your own infrastructure via IaC scripts is that many configurations are included in the code and your dependency on manual administration based on expert knowledge is reduced. When scripts are updated, the changes to the resources are summarised clearly for the administrator, which can prevent unwanted changes such as misconfigurations and downtimes. In addition, versioning makes it easier to carry out rollbacks. Reusability is also increased and deployment speeds are reduced, as the script can be used to deploy environments multiple times and the configured resources can be transferred more easily to other application scenarios. The possibility of multiple deployments allows development environments to be set up as required with production scripts, further scripts could be stored in public repositories, e.g. those that fulfil the complementary criteria for customers of the C5 criteria catalogue and thus support the implementation of security requirements for users.

advantages of a landing zone in the context of IaC

A landing zone is a service in the cloud that enables a multi-account structure for larger organisations so that various tasks (e.g. development, operation, audit) are carried out with minimal rights. Within the zones, users can only use predefined services and IaC templates, which enables basic security. In addition, guidelines can be defined that prevent certain configurations or send alarms in the event of non-compliance. According to the cloud providers’ specifications, landing zones should also be provided with IaC so that they are traceable and changes are easier to recognise. This technology also opens up new opportunities for regulators to specify requirements for the organisations concerned and check them in a scalable manner. To summarise, the advantages of IaC can be extended by additional services and scripts can also support the secure provision of these services. In summary, IaC can support authorities and companies in the secure use of the cloud, as the code-based approach makes security configurations easy to check and prevents misconfigurations.

By Jan Bings, Division Virtualization and Cloud Security

By Jan Bings, Division Virtualization and Cloud Security

Further information on the Cloud Computing Compliance Criteria Catalogue C5:

https://www.bsi.bund.de/dok/7083384
Infinite Expanses – and Why They Need Global Rules

Cyber Security for Space Infrastructures Can Only Work Together

By Frank Christophori and Dr. Johanna Niecknig, Division Air and Space IT Security Systems

Satellites dominate the digital networking of society, the economy and states worldwide. Maritime or air-borne applications for intercontinental flights rely exclusively on satellite-based services for navigation and communication. Also, global climate research and reconnaissance are inconceivable without satellites. In principle, satellite operations and services do not depend on unique nations only. To succeed with cyber security for space systems a crossborder approach is mandatory.

The dependencies on space-based systems continue to grow rapidly. In the context of New Space, the commercialisation of space travel, the number of objects (especially in low-earth orbit) and stakeholders involved is exploding. However, this also alarmingly fast increases the risk of cyber attacks on satellite systems – especially causing a great deal of damage with manageable effort. At the same time, it is difficult or impossible to attribute the attackers in cyberspace. Specific cyber security standards are therefore urgently required. In principle, satellite operations and services do not depend on unique nations only. To succeed with cyber security for space systems a crossborder approach is mandatory.

The BSI supports the European Commission in coordination within the BSI makes it possible to utilise synergies between the state, industry and research on single hand and international partners on the other – with the aim of jointly shaping the topic of cyber security for space systems and implementing measures worldwide.

SATELLITE SYSTEMS AS CRITICAL INFRASTRUCTURE

An essential question in this context is the extent to which satellite systems are or will become critical infrastructures in accordance with the KRITIS Regulation. With the implementation of the European Network and Information Security Directive 2 (NIS2) space is considered a critical sector in its own right; but limited to the ground segment. Furthermore, only operators of the segments named in the NIS2 or KRITIS Regulation is obliged to implement dedicated security measures and to submit the required evidence to the BSI as the competent authority. This ignores completely the development and construction phase of the satellites. Therefore, it is essential to find a way to handle the systems in orbit. Internationally, nations often refer to satellites as National Critical Functions (NCF), as they make a critical contribution to the defined KRITIS sectors, particularly in terms of their availability. In contrast to a critical infrastructure, however, there is no specific legal basis for an NCF.

The BSI is currently cooperating with various partners worldwide on the topic of standardisation, regulation, KRITIS versus NCF, and is playing a leading role in this area. The coordination of activities within the BSI makes it possible to utilise synergies between the state, industry and research on the one hand and international partners on the other – with the aim of jointly shaping the topic of cyber security for space systems and implementing measures worldwide.

Further information:


In Focus: Cooperation Based on Trust

A Dialogue with the Chairs of the ENISA Management Board

The European Union Agency for Cyber security (ENISA) was established to ensure a high common level of cyber security among EU member states. ENISA's strategic direction and priorities are determined by the Management Board. In autumn 2023, Fabienne Tegeler, Head of Section at the BSI, took over the chairmanship of the Management Board from Jean-Baptiste Demaison from France. In this interview, the two discuss challenges facing ENISA and new goals.

What are the major challenges for ENISA?

Jean-Baptiste Demaison: In view of the constantly tense threat landscape in cyberspace, the greatest challenge for ENISA remains promoting and harmonising the level of cyber security in the European Union to be prepared for the next significant cyber incident in Europe. This can be achieved through continued support to Member States in developing their national capabilities and by encouraging efficient intergovernmental coordination.

Fabienne Tegeler: We are facing a growing number of tasks for ENISA, combined with increasing threats and challenges in cyberspace and additional legislation at the European level. We must ensure that ENISA's profile as the EU agency for cyber security remains clear.

What role does the Management Board play here?

Demaison: The Management Board sets ENISA's strategic direction and priorities and ensures that ENISA conducts its business in accordance with its mandate and EU legislation. Moreover, the Management Board is a community of cyber security leaders from the Member States contributing to fostering trust among them and promoting common perspectives.

Tegeler: If you mirror the relationship between Germany and ENISA at national level, what similarities do you see?

Demaison: ANSSI has always participated actively in ENISA's working groups, providing support through contributions to studies, conferences, specialist publications and more. We greatly value the role of the National Liaison Officer as the central SPOC acting as a multiplier from ENISA to the BSI and vice versa. The BSI also has two Seconded National Experts (SNE) at ENISA, i.e. BSI employees who work at ENISA for a period of two to four years, fostering trust and exchange.

How does the BSI work together with ENISA?

Demaison: My two main goals and, hopefully, achievements, since I became Chairperson were: Transforming the Management Board into a more efficient strategic leadership body, by introducing strategic man-agement board meetings. Secondly, I worked towards developing the Agency into a state-of-the-art platform for cyber security expertise in all its dimensions, leveraging the capabilities and knowledge of the member states. This shift aimed to position ENISA more prominently at the forefront of shaping and implementing EU cyber security policies.

Tegeler: We greatly value the role of the National Liaison Officer at all levels of government to promote cooperation. ENISA significantly contributes to harmonising the level of IT security in the EU, while respecting the differences between the 27 member states. The idea of establishing a central office function in the federal-state relationship at the BSI at national level is very similar: we aim to work together more closely, avoid duplication of work and reduce bureaucratic and legal hurdles. Both at the European and national level, the goal is not to shift competencies for implementing IT security to the next higher state level.

What role should ENISA play in the EU in future?

Demaison: ENISA has a key role to play in strengthening the cyber security of the Union. This role should be further reinforced through adequate resources and cooperation with all relevant partners.

Tegeler: I am very pleased that the BSI and Germany are taking on this role for the first time. I aim to actively contribute to better coordination and integration of the bodies dealing with cyber security at the European level. It is also important to me to continue the good and constructive culture of discussion, in which every voice matters, regardless of the size of a member state. In the coming year, the evaluation of the Cyber Security Act/ENISA mandate will be an important task for me and my deputy Stefan Lee.

How does ANSSI work together with ENISA?

Demaison: If you mirror the relationship between Germany and ENISA at national level, what similarities do you see?

Tegeler: I see parallels here. Coordinating units are necessary at all levels of government to promote cooperation. ENISA significantly contributes to harmonising the level of IT security in the EU, while respecting the differences between the 27 member states. The idea of establishing a central office function in the federal-state relationship at the BSI at national level is very similar: we aim to work together more closely, avoid duplication of work and reduce bureaucratic and legal hurdles. Both at the European and national level, the goal is not to shift competencies for implementing IT security to the next higher state level.

What role should ENISA play in the EU in future?

Tegeler: ENISA has a key role to play in strengthening the cyber security of the Union. This role should be further reinforced through adequate resources and cooperation with all relevant partners.

If you mirror the relationship between Germany and ENISA at national level, what similarities do you see?

Tegeler: I see parallels here. Coordinating units are necessary at all levels of government to promote cooperation. ENISA significantly contributes to harmonising the level of IT security in the EU, while respecting the differences between the 27 member states. The idea of establishing a central office function in the federal-state relationship at the BSI at national level is very similar: we aim to work together more closely, avoid duplication of work and reduce bureaucratic and legal hurdles. Both at the European and national level, the goal is not to shift competencies for implementing IT security to the next higher state level.
The View Across the Big Pond.

We Need to Place the Topic of Cyber Security on the Agenda Prominently.

Claudia Plattner, BSI President, on her trip to Washington, D.C., and San Francisco in the USA

In early September, the BSI embarked on a week-long journey to the US, bringing along a multitude of topics: Harmonising standards, establishing a vibrant ecosystem for digital products, discussing the cyber security agenda, developing a better situational picture, discussing the impact of the CRA and the question of how do we prominently place cybersecurity on the agenda?

My series of appointments started on Monday evening with the Internet Security Alliance (ISA) Industry Dinner. There I had the opportunity to thank Larry Clinton, the head of the ISA, for the good cooperation on the internationally published handbook „Managing Cyber Risks“. We also used the dinner to anchor the topic of cyber security in the business world.

On Tuesday morning, during a visit to the German Embassy, discussions revolved around the US cyber security strategy released in March. It is enviably specific and well worth looking at. For example, it stipulates the initiation of a US IT security label. The Federal Communications Commission (FCC) will implement it, allowing the first labels to be issued by the end of 2024. Similar to our agreement with Singapore, our goal is to achieve harmonisation with our IT-SiK. With these labels, we are offering users a decision-making criterion by the end of 2024. Similar to our agreement with Singapore, our goal is to achieve harmonisation with our IT-SiK. With these labels, we are offering users a decision-making criterion when purchasing IT products – security at a glance – while also giving manufacturers a clear competitive advantage. A classic win-win situation.

Later that morning, I met Jen Easterly, Head of the Cyber Security and Infrastructure Security Agency (CISA). A fascinating personality: she is a Rubik’s Cube enthusiast, has degrees from West Point, a Master’s in Philosophy, Politics and Economics from the University of Oxford and spent 20 years in the US Army. In our discussions, we covered topics such as the US cybersecurity strategy. CISA incorporates some aspects of the strategy’s implementation plan released in July, including the improvement of information sharing among sector-specific supervisory authorities.

In the afternoon, the journey continued to the White House to meet with Kemba Walden, the acting National Cyber Director of the US. We discussed, among other things the 69 high impact initiatives of the US cyber security strategy implementation plan. These initiatives aim to achieve the key requirement for close collaboration between the public and private sector. From these meetings, I took away two key facts that are essential to advancing the topic of cyber security:

Firstly, it requires people like Jen and Kemba who can inspire and act authentically. Secondly, open and transparent dialogue is crucial.

On Wednesday morning, I met Jim Lewis, Senior Vice President and Pritzker Chair of the Centre for Strategic and International Studies (CSIS). One insight gained was that the cooperation between the government and the private sector will need to change. We require specially tailored support and information services to anchor cyber security in line with demand.

During the Billington Summit, I repeatedly felt a lot of sympathy for Germany. The organiser of the conference, Tom Billington, is planning a trip to Germany. An opportunity for us to give him an insight into our work. He also revealed himself as an ambassador for the topic of cyber security. On the panel, we discussed ways in which individual countries can build up their cyber defences through cyber security programmes. My favourite: Politics, business and science must work together to create an environment in which state-of-the-art technologies can ensure cybersecurity.

On Thursday, I met Paul Nakasone, Director of the NSA, and his team. I had the chance to see the Cyber Security Operations Centre and see how they work together with other cyber security forums. During a round table with analysts, I highlighted our cooperation on cryptography and certification, among other things. For me, a transparent dialogue is crucial for comprehensive situation monitoring.

Before heading back home, I took a detour to San Francisco: we kicked off our joint project work with the German Centre for Research and Innovation. Together with science, business and the public sector, we want to utilise the opportunities that arise from AI, for example. This will enable us to promote research and innovation in a targeted manner.

In retrospect, what has stuck with me is how “vibrant” the cyber ecosystem in the USA is. It is therefore important to me to create a similarly vibrant ecosystem in Germany, in which:

- products are so user-friendly that administration, business and society actually use them,
- there are needs- and user-orientated support and information services and
- a transparent exchange between the individual players forms the basis for cyber security.
European Exchange for More Cyber Security in Digital Administration

At the VIS!T Symposium of Cyber Security Authorities in Luxembourg, the BSI Presented Insights into Secure Digital Administrative Processes

By Clarissa Wilkie, Division International Relations

Under the motto “Digital administration, but please not without cyber security”, experts from cyber security authorities and public administrations from five countries gathered to share insights. The BSI participated with multiple contributions, sharing experiences and insights on IT baseline protection, the use of clouds in administrations, and European cooperation.

Every two years, the cyber security authorities from Germany, Austria, Switzerland and Luxembourg invite decision-makers and IT specialists from public administrations to exchange ideas and network. For the first time in 2023, the Principality of Liechtenstein also participated. The BSI contributed, among other things, with presentations on IT baseline protection, the secure use of clouds in administrations and cross-level cooperation in Germany and Europe.

**IT BASELINE PROTECTION IN THE FEDERAL ADMINISTRATION**

Dr Astrid Schumacher, Head of the section for “Information and cross-level cooperation in Germany and Europe,” emphasised that cyber security is a crosscutting issue impacting government, economy and society equally. Cyber security in a federal state is both a horizontal and vertical crosscutting issue. As a crossdepartmental, interdisciplinary authority, the BSI already takes this into account. In federal states such as Germany, however, there is an added vertical dimension, as public administration largely falls under the responsibility of the federal states. Thus, cyber security in a federal state is both a horizontal and vertical crosscutting task.

**EXCHANGE AND KNOWLEDGE TRANSFER**

Dr Astrid Schumacher presented the project “Repositioning IT-Grundschutz (IT-Basic Security)” (see article on p. 48) is under development, a significant slimmed-down entry level IT baseline protection. This should make it easier for very small institutions in particular to implement the minimum necessary security measures.

In this context, it is important to highlight platforms such as the network currently being set up for the federal IT steering body (ISB) or the municipal IT-SiBe forum. Currently the BSI project “Neue Wege in die Basis-Absicherung” (New Paths to Basic Security) (see article on p. 48) is under development, a significantly slimmed-down entry level IT baseline protection.

**IT-Grundschutz**, which is tailored towards the needs of users, therefore remains the right tool for simple and efficient information security management.

**AMENDMENT TO THE CONSTITUTION UNDER DISCUSSION**

The federal government is currently working on creating the basis for cross-level cooperation. An amendment to the constitution is under discussion with the aim of assigning a coordinating role to the BSI and creating the legal framework to support the federal states.

**CONCLUSION AND OUTLOOK**

This year’s symposium once again provided the BSI participants with the opportunity to exchange ideas with their counterparts in German-speaking countries and discuss current developments. Particularly in the face of this pivotal time, such collaboration strengthens the cooperation among cyber security authorities. Overall, the VIS!T Symposium remains a valuable format, fostering mutual learning within the German-speaking region and facilitating the exchange of best practices and collaboration opportunities. The next VIS!T Symposium will take place in Austria in 2025.

**EUROPEAN EXCHANGE AND KNOWLEDGE TRANSFER**

In his presentation on cross-level cooperation in Germany and Europe, Horst Samsel, Head of the BSI’s Directorate-General “Consulting for the Federal, State and Local Governments,” emphasised that cyber security is a crosscutting issue impacting government, economy and society equally. Cyber security runs horizontally through all political areas, such as transport, healthcare, administrative digitalisation and telecommunications. Effectively implementing cyber security requires treating it as a horizontal cross-cutting issue. As a crossdepartmental, interdisciplinary authority, the BSI already takes this into account. In federal states such as Germany, however, there is an added vertical dimension, as public administration largely falls under the responsibility of the federal states. Thus, cyber security in a federal state is both a horizontal and vertical crosscutting task.
A Success Story with Potential

The IT Security Label introduced in 2022 creates transparency for consumers. In this interview, Sandro Amendola, Head of Directorate-General Standardization, Certification and Cyber Security of Telecommunication Networks at the BSI, talks about milestones and future plans.

The first IT Security Label for a product was awarded in February 2022: Is the IT Security Label (IT-SiK) a successful model?

Sandro Amendola: The voluntary IT Security Label was introduced to make the security of IT products more transparent and easier to understand for consumers. It was clear from the outset that IT security is not static. We have managed to integrate a dynamic component into the label, which differentiates the German label from other consumer labelling schemes. By scanning a QR code, consumers gain access to current security information that can be updated as required. This is particularly important for IT products, as their security features can change over time. This is why we also check the devices and services over their lifetime through the BSI Market Surveillance and not at a single point in time when the labels are issued. This inspection is then carried out on either a routine basis, e.g. by sampling, or on an ad hoc basis, e.g. when vulnerabilities become known.

For me, the IT Security Label is therefore a success. I also feel confirmed in this by the positive response from business and consumer protection associations and the experiences of previous label holders. However, it is important to me that we do not rest on our laurels and continue to develop the label so that it continues to point the way forward in the future.

In your opinion, what are the most important milestones that the IT-SiK has reached so far?

Amendola: The first milestone was, of course, the first label issued. The application came a few days after the launch of the labelling scheme. The handover then took place during the 18th German IT Security Congress in February 2022.

Equally important for us was the introduction of the “smart consumer devices” product category at the end of 2022, which enabled us to offer the IT Security Label for a large number of products. Since then, it has been possible to apply for an IT Security Label for many different networked IoT devices. The label has also made it onto the international stage, and we were able to conclude a mutual recognition agreement with Singapore in October 2022. This confirms the importance of the IT Security Label as a blueprint for the design of European and international labels.

A particular highlight this year was the IT Security Label booth at IFA, the world’s largest trade fair for consumer electronics and household appliances. Here we aroused the interest of manufacturers and received a lot of encouragement from consumers.

Since October, interested manufacturers have been able to apply for the IT Security Label digitally via the portal for the Federal Online Access Act. This simplifies the administrative process even further and enables seamless communication in the application process.

What feedback have you received from manufacturers and consumers?

Amendola: We have received positive feedback from businesses and consumer protection organisations. This confirms that the IT Security Label is attractive for manufacturers on the one hand and is perceived as added value for consumers on the other. We received a lot of praise from consumers at the IFA. Most were surprised that such a label did not exist before and would like to see it become more widespread. Consumers particularly like the transparency on the subject of IT security and welcome the fact that a market surveillance checks the products over their lifetime. They appreciate the easy-to-understand and up-to-date content on the dynamic product information page.

Manufacturers and service providers who have already labelled their products also report positive feedback from their customers and have noticed positive effects on purchasing and usage decisions. IT security is thus increasingly becoming a purchasing argument, so that consumers and manufacturers alike benefit from voluntary product labelling.

In order to make the IT Security Label even better known in society, we launched a nationwide advertising campaign in autumn. This will raise awareness of the topic among consumers in particular, but will of course also focus attention on products that have already been labelled.

What are the goals and priorities for the IT Security Label in the coming year?

Amendola: 2024 is particularly exciting for us, as the first evaluation of the IT Security Label is imminent. With the involvement of stakeholders from the state, business and society, we will examine how the label has proven itself and how we can make it even better in the future. We are also looking at the standards that we have selected for the label and putting the label design to the test. Of course, we are also monitoring the developments that are emerging with the European Cyber Resilience Act, a horizontal regulation in the form of a CE mark for IT products. We want the IT Security Label to be a good preparation and to offer special functional added value for consumers and manufacturers even after the introduction of a CE mark. Although we are already well positioned in this area today, we would like to expand it even further.

Manufacturers repeatedly ask us for a voluntary label for the B2B sector and a multilevel system. As part of the evaluation, we are also examining whether this is possible. Irrespective of this, we will continue to expand the areas of application for the IT Security Label; three new product categories with high everyday relevance are currently being developed. Internationally, we would like to conclude more mutual recognition agreements; we are already in talks with other nations that want to introduce similar labelling schemes.
Recognising and Understanding Consumer Perspectives

Using Evaluations for Targeted Communication in Digital Consumer Protection

by Hanna Heuer, Division Cyber Security for Society and Citizens

How do consumers evaluate information on the topic of cyber security? How do they protect their IT and their data, what experiences have they already had with cybercrime? These questions were investigated at the BSI in 2023 – on the one hand with the LEIA project, which focused on user studies on the BSI’s own consumer information, and on the other hand through the representative citizen survey “CyMon – the Cybersecurity Monitor” together with the Police Crime Prevention of the Federal States and the Federal Government (ProPK).

As a manufacturer-independent and competent technical centre, the BSI supports consumers in the risk assessment of technologies, products, services and media offerings. In addition to better protection for individuals, this also increases society’s resilience to cyber risks of all kinds. This overarching goal of digital consumer protection must be broken down into the level of information, needs and interests of the target group in day-to-day awareness-raising work. And this target group is as diverse as our country – some use the internet primarily as a means of communication, while others connect their entire home or spend their free time on social media platforms or online gaming. While some people approach the digital world with caution and seek information and support first, others test out new possibilities – sometimes light-footedly, sometimes recklessly.

This spectrum could be described in even more detail and leads to the question of how information on cyber security should be designed so that it is applicable and helpful for consumers in everyday digital life. The BSI pursued several approaches in 2023 to find answers to this question: On the one hand, it had information materials reviewed and evaluated by test subjects in a structured manner and, on the other, it asked the target group directly about their knowledge, attitudes and experiences on the topic of cyber security.

LEIA – AWARENESS MEASURES PUT TO THE TEST

The aim of the LEIA project – Longitudinal Study on Effective IT Security Awareness – was to evaluate various products for sensitising and informing consumers through user studies and thus identify potential for improving these products. By effectiveness is meant that individual communication products were analysed to determine whether they actually motivate consumers to engage with the topic, whether they understand and remember the information provided and whether they (want to) implement the corresponding measures.

The product selection for the study reflects the variety of multimedia offerings from the BSI’s consumer communication: In a studio test, test subjects evaluated two different versions of the “Creating secure passwords” website, among other things. In separate online surveys, test subjects were able to provide feedback on the consumer protection newsletter “sicher ∙ informiert” and various video formats, for example.

In order to generate comparable statements about the individual products, the project managers defined overarching metrics, so-called key performance indicators (KPIs), which were determined using a series of statements about the products. These KPIs related to the aspects of user loyalty (including “I would also recommend the medium to other people”), design (including “I really like the overall impression of the medium or the layout”) and content (including “The medium has a high information content”).

How do consumers evaluate information on the topic of cyber security? How do they protect their IT and their data, what experiences have they already had with cybercrime? These questions were investigated at the BSI in 2023 – on the one hand with the LEIA project, which focused on user studies on the BSI’s own consumer information, and on the other hand through the representative citizen survey “CyMon – the Cybersecurity Monitor” together with the Police Crime Prevention of the Federal States and the Federal Government (ProPK).

And this target group is as diverse as our country – some use the internet primarily as a means of communication, while others connect their entire home or spend their free time on social media platforms or online gaming. While some people approach the digital world with caution and seek information and support first, others test out new possibilities – sometimes light-footedly, sometimes recklessly.

This spectrum could be described in even more detail and leads to the question of how information on cyber security should be designed so that it is applicable and helpful for consumers in everyday digital life. The BSI pursued several approaches in 2023 to find answers to this question: On the one hand, it had information materials reviewed and evaluated by test subjects in a structured manner and, on the other, it asked the target group directly about their knowledge, attitudes and experiences on the topic of cyber security.

TIPS ON USER-FRIENDLINESS ALREADY IMPLEMENTED

The surveys carried out have shown that the evaluated products have already achieved good scores for all KPIs. This applies in particular to the content. As a result, the aim is to maintain the level of topicality, information content and trustworthiness of the sender. The BSI can emphasise even more strongly how relevant cyber security is and should be in everyday digital life. For some products, findings from the surveys have already been implemented with regard to user-friendliness; for others, this will be done on an ongoing basis. As a flyer with “Tips for a Secure Home Network” was tested as a prototype, some adjustments could be made to the design before going to print for the events “Open Day of the Federal Government” and “Gamescom” in August 2023. The monthly recordings for the “Update available” podcast have now been removed from some of the content elements. And positively evaluated design elements from the website test will be deliberately taken into account when revising or planning topic pages in the consumer area on www.bsi.bund.de.
Another perspective, which is also an important working basis for the BSI's consumer communication, is provided by "CyMon – the Cyber security Monitor". The representative online survey, which has been conducted and published annually since 2019 under the name "Digital Barometer" by the BSI and the Police Crime Prevention of the Federal States and the Federal Government (ProPK), focuses on information behaviour, attitudes and knowledge on the topic of cyber security as well as experiences in the area of cybercrime. In 2023, a new call for tenders was issued, which, among other things, increased the number of people surveyed and involved a comprehensive revision of the questionnaire. BSI and ProPK took this as an opportunity to change the name of the survey: Under the title "CyMon – the Cyber security Monitor", the focus on cyber security now takes centre stage.

INFORMATION AND PROTECTION BEHAVIOUR

The 2023 results show that a good half of respondents at least occasionally inform themselves about cybersecurity. The relevance of the topic varies greatly depending on usage behaviour and is considered particularly important when it comes to financial transactions (online banking). When it comes to personal data and the means of communication used – from email communication to social networks, messengers, video conferencing and learning platforms – cyber security is in some cases significantly less important in descending order. On average, respondents use four of the cyber security measures surveyed to protect themselves against cybercrime. Up-to-date antivirus programmes (66%) and secure passwords (63%) are particularly well known and are also used most frequently (54% and 53% respectively).

EXPERIENCE WITH CYBERCRIME

More than one in four people have been affected by cybercrime (27%). Around four in ten of those affected (44%) have experienced such a criminal offence at least once in the past twelve months. If these incidents are summarised in overarching categories, data theft (33%), fraud in general (32%) and online shopping fraud (27%) were the most frequently experienced offences in the past twelve months. Overall, eight out of ten people have suffered damage as a result of cyber attacks in the past year (80%). This primarily involved loss of trust in the relevant online services (33%), time-related damage (26%), emotional damage such as offence or fear (23%) and loss of data (22%). Almost one in five (18%) suffered direct financial damage.

CONCERNS ABOUT FRAUD THROUGH ARTIFICIAL INTELLIGENCE

CyMon also included several questions on the current topic of artificial intelligence (AI). This revealed that almost all respondents had already heard of AI (98%) – six out of ten respondents also stated that they knew exactly what the term meant (60%). Many have already heard of criminal methods in which AI is used. However, attacks on AI applications are comparatively little known. In addition, a clear majority of respondents are very concerned about possible manipulation or fraud by AI applications.

The results of CyMon will be taken up in the first quarter of 2024 in particular, in which digital consumer protection is a particular focus for the BSI in terms of communication, and will be taken into account when addressing consumers.
Step by Step to a Guest Wi-Fi

Do you actually have an overview of who you have already given your Wi-Fi password to? A separate Wi-Fi for guests creates order and separates your online activities from those of your visitors. The highlight: the extra network can be set up on modern routers in just a few simple steps and at no extra cost.

WHAT A SECOND NETWORK AT HOME IS CAPABLE OF

A guest Wi-Fi is a wireless network connection that can be set up in addition to the existing home network. As soon as you have activated a guest Wi-Fi, you have two separate networks.

A separate Wi-Fi for guests has several advantages:
• Guests can hardly cause any damage to the actual home network. Even if, for example, malware is found on a guest’s laptop or smartphone and the visitor connects to your guest Wi-Fi, your data remains secure. This is because you process online banking or send personal data in your secure primary network.
• You can assign permissions, e.g. specify which pages may be visited or how much bandwidth is available. This means you can determine which functions your guests are allowed to use and thus retain control over your Internet connection.
• It is practical in everyday life: routers often offer the option of creating a QR code that your visitor can simply scan to gain access to the network.
• The guest Wi-Fi or a separate Wi-Fi is also useful to integrate smart devices. A possibly insecure robot vacuum cleaner or a roller shutter control that has not been set up accordingly can cause less damage there.

SET UP THE WIRELESS NETWORK FOR GUESTS

Before you set up the guest Wi-Fi, ask yourself the question: “What kind of router do I have?” Although the instructions below work for the most common models, it is possible that menu items are named differently, can be found under different settings or that functionalities are missing.

It is possible to activate a network for guests at any time, even after the initial setup of the router. This means that you can switch the additional Wi-Fi on and off whenever you want.

1) Open the settings of your router. This works either via a short address specified by the manufacturer or via an IP address that you enter in your internet browser. This is often 192.168.0.1 or 192.168.178.1, for example.
2) Select the menu item “Wi-Fi” (this item can also be called “Network” or “Guest network”) and click on “Guest access”.
3) Activate guest access here, usually by ticking or sliding a box.
4) Now assign a name for your new network that does not allow any conclusions to be drawn about you, other people or the router model.
5) Assign a strong password. The password can be long and complex because your guests usually only enter the password once and can then save it for the next visit. For this reason, the Wi-Fi password should consist of at least 20 characters without any correlation.
6) Check whether you can also set the encryption of the connection here. This should be at least WPA2 – if possible even WPA3.
7) Confirm the settings. You can now share the access data with your guests. At the same time your actual home network remains protected. You should also integrate smart devices such as robotic vacuum cleaners, roller shutter controls or intelligent doorbells into this separate network and thus separate them from sensitive services such as online banking or home office applications.
PASS ON ACCESS DATA SECURELY

There are many ways to share the password for the guest Wi-Fi with friends and family, but not all of them are secure. The most important rule is: only share Wi-Fi passwords with people you trust. Here are four ways to give guests access to your network:

• First things first: don’t post your login details anywhere, only give out access on request.

• The classic solution: write the Wi-Fi password on a piece of paper and store it safely out of sight. This way, your guests can type the password directly from the piece of paper.

• The convenient option: Let your router generate a QR code that your guests can then simply scan. This way, guests can’t make a mistake.

• Without paper: Modern smartphones can share Wi-Fi passwords with neighbouring smartphones (with the same operating system).

If these instructions are not suitable for your device, your operating system or your individual problem, we recommend that you check with the respective manufacturer or provider to possibly find even more specific help there.

Further information:
https://www.bsi.bund.de/dok/10651618
https://www.bsi.bund.de/dok/6596788

Order your BSI Magazine

Twice a year, the BSI Magazine “Security in focus” offers insight into national and international cyber security, 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
SAVE THE DATE
7 - 8 May 2024
The BSI Invites You to the 20th German IT Security Congress!

On the two days of the congress, live lectures, panel discussions and virtual exhibition stands will bring IT security to life and provide a comprehensive technical insight into current cyber security topics. The event takes place in digital form and offers participants a platform for dialogue.

Register now in advance via the congress website and be informed about the activation of the registration portal!
www.bsi.bund.de/IT-Sicherheitskongress