BSI Magazine 2019/01

Security in focus

The BSI as a Competence Centre and Service Provider
Private Matters Must Remain Private

When this BSI magazine is published, the so-called “politician leak” (see article on page 18), in other words the publication of extensive private data on celebrities and politicians on the Internet by a 19-year-old hacker from Hesse, dates back a good four months. In the meantime, even more leaks and hacks have been reported by the media. And there have probably been more leaks and hacks that the media have not yet reported on.

Do we have to get used to this? Do we have to accept that cybercrime of whatever origin and the violation of the constitutionally protected private sphere are an inevitable part of everyday digital life? I would say that we don’t. But we will have to change our behaviour. We will have to learn to protect ourselves better. And we need to strengthen the protection mechanisms.

In the analogue world, no one leaves their home or apartment without locking the door. Nobody would park their car at the airport and leave the key in the ignition either. And we certainly wouldn’t send our tax return to the tax office in an unsealed envelope. In the digital world, however, we do all of these things. We let ourselves be read like an open book, with the repeated argument that we have nothing to hide.

But, we do. Even if millions of users want to share their lives, their thoughts, their photos with other Internet users, even if they are willing to have their coordinates evaluated around the clock, they have a right to the protection of their privacy. And even if, as in this case, the perpetrator has probably collected most of the data from publicly available sources and only illegally obtained it in a few cases, its publication remains a criminal offense.

Personal data is a highly interesting target for cyber attacks. It starts with the phone number or email address and doesn’t stop with private photos and account numbers. We must protect this data from all perpetrators and all motives.

We at the BSI will therefore intensify our efforts to inform all users about the necessary protective measures to protect their privacy on the Internet. We will establish digital consumer protection as quickly as possible in order to provide them with decision-making aids when purchasing products. We will further refine our instruments and methods to detect attacks as early as possible. And, together with the other security authorities, we will search for and find the perpetrators. So that the Internet becomes a secure space in which we can all enjoy the benefits of digitalisation.

Sincerely yours,

Arne Schönbohm,
President of the Federal Office for Information Security

“We at the BSI will intensify our efforts to inform all users about the necessary protective measures to protect their privacy on the Internet.”
# News

4  In Brief

## Cyber Security

6  Making Home Networks More Secure
10  SAT Solvers Can Help – Propositional Logic’s Satisfiability Problem
14  Who Actually Ensures Cyber Security in Germany?
18  Theft and Illegal Publication of Politicians’ Personal Data

## The BSI

20  Designing Information Security
24  Good Grades – Online Customer Survey
26  A Day at the BSI
28  Here’s to a Good Partnership – The BSI and the Federal States

## Digital Society

30  Compactly Tested – Security Analysis of Data Centres
32  Artificial Intelligence in IT Security – Competence Centre in the Making

## BSI International

34  Joining Forces to Ensure Secure Information Technology – VISIT Attracts Many Participants from the German-speaking Regions
36  The New Mandate of ENISA – A Cyber Security Institution in Transition

## IT Security in Practice

38  In Case of Suspicion: X-ray – Manipulation of IT Hardware
40  IT-Grundschutz Profiles: Information Security for SMEs
42  Made-to-measure Security – Increasing Cyber Security in the German Craft Sector
44  Basic Tip: Higher Security on the Internet for Citizens

## And Finally

46  Events in 2019
47  Subscription Order Page
51  Legal Notice
Security for Federal Networks

On 30 November 2018, the President of the BSI, Arne Schönbohm, and Andreas Gegenfurtner, President of the Federal Agency for Public Safety Digital Radio (BDBOS), signed the administrative agreement on long-term cooperation to ensure the security of the Federal Networks (Netze des Bundes, NdB).

The BDBOS took over the Governmental Networks on 1 January 2019. It is thus responsible for the planning, construction, operation and safeguarding of the functioning of the government network. To this end, the federal agency will gradually relieve the previous technical operator, T-Systems, of its responsibilities.

For more information see https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/verwaltungsvereinbarung_bdbos_bsi.html

Alliance for Cyber Security

Enabling the exchange of experiences regarding challenges in cyberspace and benefiting from the expertise of others – that is what the Alliance for Cyber Security (ACS) offers to more than 3,500 companies and institutions. This year, the activities of the ACS will be guided by the motto “Networks protect networks.” The ACS will support interested business associations in creating IT-Grundschutz profiles that offer a practical working aid for increasing cyber security in the respective industry. For the European Cyber Security Month 2019, the ACS is planning to conduct various activities with other German cyber security initiatives to increase cyber security in the private sector. Lastly, the 29th Cyber Security Day “Networks protect networks” on 26 September 2019 at Haus der Wirtschaft in Berlin promises to be a special highlight. At this interactive event, 350 participants, partners and multipliers will be able to meet successful initiatives, contribute their own expertise and expand their network. Save the date!

More information will follow at www.allianz-fuer-cybersicherheit.de
First Smart Meter Gateway Certified

On 20 December 2018, the BSI issued the first certificate based on the protection profile for the Smart Meter Gateway. The Smart Meter Gateway was developed by Power Plus Communications AG (PPC) together with OpenLimit SignCubes AG. In the test procedure, besides proving compliance with the security specifications in the device itself, the manufacturing and development processes of the manufacturer and the delivery routes of the devices were examined and finally certified by the BSI. With the certification of the Smart Meter Gateway, the first IT security label has also been awarded.

For more information see https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Erstes_Smart_Meter_Gateway_zertifiziert_201218.html

E-world in Essen

“E-world energy & water,” the leading European trade fair for the energy and water industry, took place in Essen from 5 to 7 February 2019. The BSI had a booth at the fair and provided information on intelligent and secure networking in the area of energy supply. The highlight at the booth of the national cyber security authority was a showcase that presented the functionality and security features of a smart meter gateway and the future areas of application for intelligent measurement systems.

For more information see https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/e-world2019_010219.html
Making Home Networks More Secure

Technical Guideline Defines Minimum Requirements for the IT Security of a Router
A Technical Guideline (TG) recently published by the BSI defines a minimum level of IT security for broadband routers. It is intended to increase the IT security of routers and the Internet infrastructure by establishing “Security by Design / by Default” in routers. The TG provides basic guidance for manufacturers as well as consumers.
In the course of increasing digitalisation, more and more households all over the world either own or will soon own routers. They open the door to the digital world and manage the home network, which consists of a wide variety of devices such as smartphones, printers, game consoles, refrigerators and washing machines. With the “Technical Guideline Secure Broadband Router” (BSI TR-03148), the BSI has built the foundation for greater security in home networks and the entire Internet infrastructure.

POPULAR TARGETS
The creation of the TG resulted from the events surrounding a worldwide Internet attack at the end of 2016, which also affected approximately 900,000 routers in Germany. During the attack, an attempt was made to install Mirai malware code on the routers via the remote administration interface to hijack the devices into a botnet. Mirai is a family of malware that comes in various variants such as Satori. In principle, Mirai can infect any inadequately secured Internet of Things (IoT) device. The malware often makes use of the fact that IoT devices frequently use standard passwords, which create an increased risk due to their multiple usage. After the IoT device is infected, the device is integrated into a botnet.

COUNTERMEASURES
The incident in 2016 led to the creation of a TG for routers. The project lead was given to the BSI. A test concept for broadband routers already developed at the BSI served as the basis for the contents of the TG. The initial concept for the TG was presented at the first meeting of a working group newly founded by the BSI that was attended by representatives of manufacturers, associations, authorities and society.

Within the framework of this working group, the contents of the TG were discussed controversially in a total of five sessions and two commentary rounds and its contents were finally determined. Compromises could not always be found and different interests had to be weighed. Finally, the Technical Guideline was published by the BSI on 16 November 2018. It received much praise, but also criticism, and marks the beginning of an ongoing discussion and further development of the TG.

OBJECTIVES AND FUNCTIONS OF THE TG
The TG specifies minimum requirements for the IT security of routers. It refers to core functions such as Internet access and network management. For example, the TG principally demands an update mechanism and additionally recommends the automated retrieval of security updates if users do not disable this function. This requirement and the recommendation ensure that any security gaps that occur can be closed, ideally without the user taking any active action. This is extended by the requirement that the manufacturer must specify how long the router will receive security-relevant updates that close any security vulnerabilities with a combined Common Vulnerability Scoring System (CVSS) level higher than 6.0. This prevents the exploitation of known security vulnerabilities. Obsolete insecure software is still a widespread problem in routers, as the study “Securing IoT devices – how safe is your WiFi-Router?” by the American Consumer Institute shows.

Another security problem is that standard passwords are often used for a whole class of devices. The TG therefore specifies the basic requirement to assign device-specific random passwords during the manufacturing process and thus provide an additional component for preventing the mass take over of routers.
VARIOUS POSITIONS
During the discussions on creating the TG, various opinions on the subject matter surfaced: Many network providers, for example, want to protect their network by having full control over the router firmware. This is diametrically opposed to the user’s/citizen’s demand for free handling of their device. This includes, for example, the interest of some users in being able to install non-manufacturer firmware on the router. In this way, for example, newly discovered vulnerabilities can be closed, even if the manufacturer has already discontinued support for the router.

These advantages, however, are at odds with a disadvantage, since malware can also be installed on the router by using this feature. This is neither in the interest of the user nor the network provider. The opening for non-manufacturer firmware can in certain cases generate higher costs for the provider, as it must be checked that the user’s own non-manufacturer firmware (including customer firmware) is secure. The TG therefore defines that the router can offer the possibility of importing proprietary and non-proprietary software. However, when installing non-manufacturer, non-signed software whose source cannot be verified by a router, a warning message must be displayed to users and the installation must be explicitly confirmed.

BENEFITS FOR THE BUSINESS WORLD AND SOCIETY
The TG can be used as a basis for testing or certifying various routers. In combination with a testing procedure, comparability with regard to the security performance of different routers for the consumer can be achieved – and the consumer can be informed about the state-of-the-art technology. This enables users to develop a better understanding and awareness of IT security.

Ultimately, the router builds a barrier between the public and private network. It is the heart of a digital household and one of the central building blocks of digitalisation. It will become more and more important in the foreseeable future with regard to a full interconnection of the environment and the spread of the IoT. Therefore, an adequate level of IT security for routers is very important and an important step in the right direction has been taken with the creation and publication of the TG.

For more information see
The solution of Satisfiability Testing (SAT) (see info box) is critical to information technology – and therefore to IT security. Computer science is based on the principle of the correctness of algorithms. This can be proven, for example, by source code analysis. Statements forming an algorithm can be broken down to propositional logic and their correctness verified with an SAT solver.
Safety-critical software used, for instance, in aviation, nuclear facilities, the automotive industry and medical technology must be tested against the strictest standards (e.g. DO-178B) and can be automatically tested using special software tools based on SAT solvers. These tools can reliably check millions of lines of program code in high-level computer languages for errors and security vulnerabilities within a few hours. Today’s SAT solvers can solve problems with many millions of clauses and several hundred thousand variables in a manageable amount of time on multicore workstation computers.

SAT SOLVERS IN USE
SAT solvers are versatile tools that are used in a wide range of industrial applications. Their use ranges from the routine verification of the correctness of properties in complex, dynamically reconfigurable circuits during the automated hardware planning and production process to the search for weak points and errors in the automated source code analysis of complex, security-relevant software products (model checkers, SMT tools, theorem provers).

The solution efficiency of SAT solver methods in coping with complex problems has developed exponentially over the last two decades. The fact that the most efficient SAT solvers are developed as open source tools and are openly available as source code has also contributed to their rise. Algorithmic improvements become available for discussion by developers and users through free publication in technical journals. In this way, various suggestions can be exchanged on how solvers can be further developed and extended with the vast practical experience of a large, diverse user group testing solver usefulness from many perspectives.

SAT SOLVERS IN COMPETITION
Many of the SAT solvers developed as open source regularly take part in the now renowned international SAT solver competition. The event is hosted by the annual International Conference on the Theory and Application of Satisfiability Testing. Numerous application cases from industry, development, research and (since 2000) cryptography are compiled, analysed and critically assessed.

Solvers only qualify for the competition by solving application-related problems in the fields of hardware and software verification, cryptoanalysis, bioinformatics and others within a limited computing time. The solvers are then evaluated according to how

In mathematics, Boolean satisfiability (named after British mathematician George Boole) is a decision problem that can be represented by a propositional logical formula containing AND, OR, NOT combinations of binary variables only. The formula is divided into smaller logical statements, or clauses, which are then all linked to the overall formula with AND. The satisfiability problem decides whether a given quantified Boolean formula without free variables is true or false. We therefore look for an assignment of the variables with TRUE or FALSE that fulfils all clauses of the problem, or for proof that no such assignment is possible, meaning at least one clause cannot be fulfilled.
reliably and quickly they can solve the compilation of application cases. These competition events with discussions between experts and users strengthen the exchange of ideas, motivate new developments and underpin the confidence of users in solvers, whose code and performance transparency ultimately provide a kind of quality assurance, open to anyone interested.

SAT SOLVERS AND NP PROBLEMS
In computer science, a problem is called NP-complete (complete for the class of problems that can be solved non-deterministically in polynomial time) if it belongs to the most difficult problems in the NP class (both NP and NP-hard). The satisfiability problem – the first recognised NP-complete problem – is also the core of a large class of NP-complete problems and is central to the investigation of Artificial Intelligence (AI) systems. Most decision and optimisation problems in AI, knowledge representation and decision reasoning are notoriously difficult to solve, their complexity exceeding NP. Despite their intractability in the classical sense, these problems can be solved with surprising effectiveness in practice across many areas using solution methods based on SAT and integer programming solvers.

Using an SAT solver and a supercomputer, computer scientists Marjin Heule and Oliver Kullmann solved difficult mathematical problems, including the 3,700-year-old number puzzle of the “Pythagorean Triple” in 2016. The question was: Is it possible to divide the natural numbers from 1 to n into two groups so that neither of them contains a Pythagorean triple? That meant all three numbers of a triple should not belong to the same group. Increasing n quickly complicates the number of division possibilities, with 2^n possibilities meaning that n = 100 already renders more than 10^30 possibilities to evaluate. The two researchers were able to prove that a solution is only possible up to n = 7824. Trying all 2^7825 possibilities blindly would mean testing 4 × 10^2355 combinations, a task no modern supercomputer could accomplish in its lifetime.

Solving this problem with an SAT solver means converting the question under consideration into a satisfiability problem. That is by no means a trivial task, and its result can be variously parameterised. One and the same question can be converted into several logical formulas that differ in terms of the number of binary variables and the length and number of clauses.

The format of the logical formula of the solver input plays an important role in the solver’s efficiency, depending on the solver settings.

SOLVING THE SATISFIABILITY PROBLEM WITH THE SAT SOLVER CRYPTOMINISAT
The source code of the open source SAT solver CryptoMiniSat (CMS) was analysed in a project carried out by the BSI together with inducto GmbH. Through a statistical analysis of the runtime results of the solver in repeated attempts to solve instances that implement a cryptographic KPA attack on the Small AES-64 model cipher SR (3, 4, 4, 4), combinations of the CMS setting parameters were found that could solve this problem with a realistic effort, despite being generally regarded as unsolvable. The empirically determined solver para-
Meter settings were further refined using the open source SW tool SMAC for automated algorithm configuration, which uses sequential model-based optimisation, a reinforcement learning method in AI. The strong results the project achieved were presented at the FLoC (Federated Logic Conference) in Oxford in July 2018.

The SAT solver’s (CMS) statistical runtime analysis for instances of different sizes was visualised with box plots, since median and quartiles more stably measure the dispersion of the number of results than mean and variance, which are limited by longer runtimes. It should be noted that CMS operates indeterministically, running parallel on several threads and delivers different runtimes with the same inputs and identical solver settings.

The code analysis and a subsequent feasibility study lead to an increase in CMS efficiency when solving hard CNF instances using AI methods. It may sound like circular reasoning when SAT solver methods are used for machine learning while SAT solvers are improved using AI. However, computer science is already making advances in this area, producing positive results.

For more information see https://easychair.org/publications/preprint/Q4kv
Who Actually Ensures Cyber Security in Germany?

The State Cyber Security Architecture

By Dr. Sven Herpig, Stiftung Neue Verantwortung

In recent years, the number of state actors in the field of cyber security has vastly increased. It is easy to lose one’s bearings. Distributing responsibilities sensibly and finding the right contacts depends on knowing the current status of cyber security architecture in Germany.
Dr. Sven Herpig is Head of International Cyber Security Policy at Stiftung Neue Verantwortung (SNV) and brings together the experts from both sides of the Atlantic on all facets of the interior, security and defence policy in the cyber space. As part of the EU Cyber Direct (EUCD) project, he analyses the cyber-resilience policy of the European Union as well as the diplomatic EU-US relations in cyber space.

GENESIS
The starting point of the institutional structure in the area of cyber security in Germany can be dated with little doubt to 1 January 1991. This was the birth of the modern form of the Federal Office for Information Security (BSI). The linchpin of IT security in Germany, it still serves today as a central point of contact. Since then, however, the number of government actors at federal and state level addressing IT security has increased. One reason for this is the new divisions that have arisen to address new challenges. The Cyber Defence Centre (Cyber-AZ) under the BSI, for instance, was introduced with the Cyber Security Strategy in 2011, while the Central Office for Information Technology in the Security Sector (ZITiS) was envisioned in the Cyber Security Strategy in 2016 and created in 2017.

DIGITALISATION
Another reason for the rapid rise in state actor participation in recent years is digitalisation itself. Security is a central element of successful digitalisation. As significant sectors of the general public are digitalised, IT security must in turn be considered more broadly. IT security is being discussed everywhere from health care cards and critical infrastructure operators to the connected refrigerator and the (smart) city of the future. This has turned purely technical IT security – the achievement of the protection goals of confidentiality, integrity and availability – into cyber security. Many dismiss it as a new-fangled term, but cyber security encompasses much more than mere technical security. Besides achieving protection goals, it also includes political, legal, social and cultural dimensions. Digitalisation together with the evolution from IT security to cyber security not only necessitates new agencies, but also brings a rising number of agencies into the cyber security discussion that previously had little or nothing to do with IT security. This includes the Federal Ministry of Justice and Consumer Protection (BMJV) and the Federal Financial Supervisory Authority (BaFin).

CYBER SECURITY ARCHITECTURE
The entirety of all institutions involved in cyber security in Germany can be described as “cyber security architecture.” This architecture was not planned on the drawing board. Its development is closer to that of a typical German city, growing over a long period of time, being constantly added to when needed. While there is certainly a strategy behind each institution in this structure, there was no master plan for the complete architecture. This is hardly surprising, as the institutional structure has developed parallel to that of cyber security.

Growing structures often lead to friction, such as responsibility conflicts and additional effort, in resource distribution, for instance. So far, Germany has used a simple but quite effective trick. At both the strategic and operational levels, a central actor (“spider in the web”) links many institutions and ensures the exchange of information and coordination. At the strategic level, this is the Cyber Security Council (Cyber-SR) and at the operational level it is the BSI, such as with its Cyber-AZ.
CONCLUSION
The development of German cyber security architecture is not yet complete. Neither is lacking an overall concept cause for great concern, even if it certainly would have been helpful. Since digitalisation is still underway and critical developments such as the diffusion of civil and military aspects in Germany (e.g. by the “Cyber-Agency”) are on the rise, a concrete strategy for German cyber security architecture must now be systematically developed. Stiftung Neue Verantwortung presented an open-ended first draft of the status of architecture and responsibilities with its paper “Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik (Responsibilities and Tasks in German Cyber Security Policy)”.

For more information see https://www.stiftung-nv.de/de/publikation/zustaendigkeiten-und-aufgaben-der-deutschen-cyber-sicherheitspolitik
Theft and Illegal Publication of Politicians’ Personal Data

On 3 January 2019, it became known that large amounts of private information from German politicians and public figures had been published illegally on the Internet since the beginning of December 2018.

WHAT HAPPENED?
The alleged perpetrator had published links to download larger volumes of data under the pseudonyms @_0rbit and @_0rbiter on the short message service Twitter. The publications were staged just like an Advent calendar. He opened another “little door” each day until 24 December and advertised new private data via Twitter, naming the person concerned.

Besides well-known public figures, German politicians, both active and former, from the EU, federal, state and local levels, in particular were the targets of the publications. The perpetrator posted personal information on these individuals on the Internet. Members of the CDU/CSU (425 persons), SPD (318), Bündnis 90/die Grünen (111), Die Linke (112) and the FDP (28) parties were directly affected. The number of indirectly affected persons, whose contact data was contained in stolen telephone directories, for example, cannot currently be quantified exactly. The phone numbers of 80% of the 994 people were published as well as the postal and/or e-mail address. Nearly 60 politicians directly fell victim to identity theft i.e. additional access data such as passwords.
Theft and Illegal Publication of Politicians’ Personal Data

and user names for certain websites were published. The data published contained both publicly accessible information, the official party e-mail address, for example, as well as private, non-public data. In some cases, even private communication content, such as family chats and pictures, was provided for download.

So far, it is unclear from which sources these data sets originated and whether the data originated from a single attack on a central service or from multiple attacks on various service providers. There are indications that the perpetrator had gathered a great deal of information from publicly available sources, also known as doxing, and in only a few cases actually obtained illegal access to personal data. The extent to which the published documents are actually authentic is subject to ongoing investigation. There is no evidence of a successful cyber attack on government networks.

WHAT ROLE DID THE BSI PLAY?

On the night of the third to the fourth of January 2019, the BSI learned of the mass publication of private information belonging to German politicians and public figures. The BSI took action immediately. A crisis team was set up on the morning of 4 January. In order to assess the extent of the problem and the potential danger, an initial review of the data published was carried out. The National Cyber Defence Centre was responsible for the central coordination of handling the case by the federal authorities involved. The BSI already notified the offices of the parties concerned on 4 January. Since then, the BSI has been in close contact with political parties and Members of Parliament and advises them individually whenever this is requested and possible.

The perpetrator stored the data packages on a number of download portals. The BSI immediately asked more than 50 of these so-called hosters, some of them based abroad, to delete the data and thus made it more difficult to disseminate it. The blocking of the Twitter accounts used was also requested and carried out by Twitter in a timely manner.

ASSESSMENT OF THE INCIDENT

Personal data and in particular access data to the online accounts of functionaries and public figures are highly interesting targets for cyber attacks. The more private life takes place on the Internet, the greater the interest in such data.

The incident makes two things clear. It shows that different motivations are possible for such acts. A foreign state does not always have to be behind extensive and sensational cyber attacks. Individual perpetrators with personal motives can also cause serious damage. Furthermore, it becomes clear how much personal data is available on the internet. The collection of publicly available information and its targeted processing also leaves those persons affected feeling a sense of unease. ■
As the Federal Government’s competence centre for cyber security, the BSI is also the central service provider for all other areas: the federal states and municipalities, large and small companies, research, manufacturers and private users. And it must act like a turntable: the faster the speed of innovation of digitalisation increases, the faster the BSI must react, keep its competencies up-to-date and ensure the transferability of the solutions found.
NOTHING WORKS WITHOUT DIGITALISATION

Digitalisation has now reached nearly all areas of our lives. Neither politics, business nor administration can do without reliable and secure communication systems. Industrie 4.0 describes the fundamental changes in the production sector, eGovernment is the buzzword for a digitalised and transparent administration. Smart home, mobile work, eHealth and self-propelled cars are yet other examples of the rapidly advancing digitalisation of the political sphere, business and private life at all levels. No end is in sight. On the contrary: Technological progress doesn’t stand still but rather accelerates over time. New technologies are introduced to the market in ever shorter time intervals and are integrated into our everyday life ever more quickly.

For users to benefit from these new technologies, cyber security must also be continuously monitored and considered in parallel – or better put: always be one step ahead – in all areas and at all levels of political, business and social life as digitalisation continues to progress. As the current situation report of the BSI and numerous security incidents demonstrate, the threat situation has also intensified and become more complex. There is still a high dynamic of attackers in the further development of malicious programmes and attack routes. With the hardware vulnerabilities they discover, there is a new quality of threat. And it can be assumed that the pace of innovation of the attackers will at least not slow down.

In recent years, the Federal Government has created the legal and strategic framework conditions with the Cyber Security Strategy, the IT Security Act, the implementation of the NIS Directive and the Digital Agenda to comprehensively counter the threat situation. As the current situation report of the BSI and numerous security incidents demonstrate, the threat situation has also intensified and become more complex. There is still a high dynamic of attackers in the further development of malicious programmes and attack routes. With the hardware vulnerabilities they discover, there is a new quality of threat. And it can be assumed that the pace of innovation of the attackers will at least not slow down.

THE BSI DESIGNS DIGITALISATION

As the national cyber security authority, the BSI designs the digitalisation process on the basis of its legal mandate. In administration, the business world and society. In order to ensure systematic support for its target audiences through targeted information, technical products and services and to take account of digital penetration, the BSI has compiled its range of services in a product and service portfolio. It addresses:

- all institutions at the federal level (ministries, authorities) that drive digitalisation projects forward or work on them,
- the Federal Government, the states, municipalities and, at the international level, bilateral and multilateral partners (EU, NATO) in the area of state/politics,
- starting with the state, operators of critical infrastructures (KRITIS), IT manufacturers, IT service providers and companies of all sectors and sizes in the economic sector, as well as political parties and party foundations and all citizens in the social sector,
- and covers everything from prevention and detection to defence against attacks on cyber security to the development of security solutions, standardisation and certification.

The product and service portfolio of the BSI includes six uniformly defined categories. Based on the “Information” category, which includes standards such as IT-Grundschutz, but also situation reports and warnings, the deployment effort increases with each category. In addition to “training and further education offers” in the field of IT security and “cooperation platforms” such as the Alliance for Cyber Security, the BSI also offers consulting services on various issues relating to the implementation of IT security. Access to the BSI’s expertise is facilitated by this clear composition in the portfolio.

FROM AUTOMOTIVE TO SMART METERS

The BSI has built up and proven its expertise in the prevention, detection and response to complex cyber attacks and IT security incidents over many years, among other ways through its responsibility for the protection of federal networks. It not only accompanies the consolidation of the federal IT system and contributes its consulting expertise
on strategic and operational issues of information security, the BSI also works together with the relevant federal ministries to shape information security in the major digitalisation projects of our time in order to ensure the functionality and added value of a society that will be heavily digitalised in the future. The spectrum ranges from the telematics infrastructure in the health sector/“eHealth” (BMG), intelligent traffic systems on land and water (BMVI), via the digitalisation of the energy system transformation (BMWi) and the Smart Home (BMWi, BMJV, BMUB) to the Internet of Things (BMI, BMWi, BMJV). In many cases, certifications are a suitable procedure to guarantee the cyber security of technical solutions, as has already happened with the Smart Meter Gateway as part of the digitalisation of the energy revolution. Certification by the BSI itself is to be regarded as the highest level. Other options are the manufacturer’s declaration to adhere to the BSI guidelines, and certification by the third-party vendor.

As an independent competence centre for IT and cyber security, the BSI ensures holistic and consistent implementation of the Cyber Security Strategy and the IT Security Law. The BSI’s National Liaison Office shapes relations with national partners in the areas of government, business and society. It advises these target audiences on the individual products and services of the BSI and records the respective demand. One special feature of the liaison system is its presence in the regions. This facilitates direct exchange and creates a concrete accessibility of the BSI on site.

Operational cooperation is established via the CERT Administrative Network (VCV). This enables the CERTs of the federal and state governments to exchange information in order to react more effectively and quickly to IT attacks. In 2018, the IT Planning Council adopted a binding reporting procedure for the exchange of information on cyber attacks, thus creating a reporting obligation between the Federal Government and the states. The BSI issues warnings, situation reports and hazard indicators via the CERT-Bund, which are fed from a wide variety of sources processed at the BSI Situation Centre. By contributing to the situation picture and supplying incident reports, the states also do their share, which is of elementary importance to obtaining a holistic picture.

The central point of contact for advice from the federal and state administrations is the BSI security consultancy. It is the central point of contact for the information security officers of the respective authorities. Through committee work, close contacts with authorities and the efficient exchange of information relevant to IT security, the employees of the security consulting division gain good insight into the situation of information security on site. The municipalities are also involved in strengthening cooperation between the Federal Government and the states. Due to the large number of municipalities, multipliers must be bundled. The BSI’s partners here are local umbrella organisations and data processing centres spanning several areas. The BSI also enables a direct connection of all municipalities to the Alliance for Cyber Security.
FROM AUTHORITIES TO CITIZENS
In the area of business and society, the Alliance for Cyber Security (ACS) of the BSI supports companies with practical assistance for the analysis of cyber risks and the implementation of appropriate protective measures under the motto “Networks protect networks.” It works closely with partners from industry and research as well as multipliers. In the meantime, as of March 2019 around 3,500 companies, public authorities, associations, research institutes and other institutions from all over Germany have joined the initiative.

The public-private cooperation UP KRITIS is available as a technical and exchange forum for all organisations based in Germany that operate critical infrastructures (KRITIS) in Germany, national trade and industry associations, recognised Single Points of Contact (SPOC) from the KRITIS sectors as well as the responsible authorities. IT security analyses and the professional discourse of the cyber security experts of the BSI with experts from industry, professional organisations and associations are an essential field of action.

The BSI’s information and consulting services for citizens are also part of the business and society sector. Since 2018, they have been extended to include the aspect of digital consumer protection. The website www.bsi-fuer-buerger.de deals with topics and information relating to IT and Internet security in such a way that they can be understood even by technical laypersons. Besides providing pure information, the BSI also provides concrete and implementable assistance. Furthermore, the “Bürger-CERT” is a free warning and information service that informs citizens and small businesses of weak points, security gaps and other risks and provides concrete assistance. Citizens can also call the free hotline 0800 274 1000 to ask questions. In the field of consumer protection, the BSI supports consumers with the risk assessment of technologies, products, services and media offerings.

FROM PREVENTION TO REACTION
As a manufacturer-independent and competent technical body, the BSI designs information security in digitalisation through prevention, detection and reaction for all players in all areas. As a competent thought leader, comprehensive initiator and central interface to the issues of information and cyber security, it makes a decisive contribution to Germany’s digital sovereignty.

This ability is based on how it works, its network thinking and the BSI’s profound technical expertise. Through its integrated cyber security value chain, the BSI uses intensive research to identify threats or gaps in existing systems, warns of them, develops new solutions and simultaneously identifies further threats. These solutions are also made available to other institutions through the cooperation between the Federal Government and the states, but also between the government, the business world and society.

The BSI actively participates in new developments in digitalised society, from Artificial Intelligence (AI) and quantum computers to the latest generation of mobile communications (5G). Through intensive cooperation, the BSI can incorporate its findings and requirements on cyber security into the development process directly and at an early stage. In the area of cryptography, it draws up recommendations and technical guidelines for cryptographic procedures and is involved in the development of international crypto standards. This bundling and networking of cyber security expertise in one authority gives the BSI its unique clout in Germany. It will also perform its additional tasks in the field of digital consumer protection and as a central certification and standardisation authority in this way: as a central and neutral service provider on IT security issues for federal, state and municipal governments, companies and citizens.
Customer requirements play a decisive role in quality management. The BSI therefore uses customer surveys to improve the quality of its work in certifying and recognising IT products.

Certifying IT products and management systems makes a significant contribution to information security in digitalisation. It depends, however, on high-quality certification and recognition procedures.

FOCUS ON QUALITY
Rising customer expectations have made quality an indispensable aspect for government. The BSI’s department “Cyber Security in Digitalisation, Certification and Standardisation” thus considers quality of critical importance, anchoring it firmly in its strategy and guidelines.

Implementing and operating a process-oriented, integrated quality management (QM) system most effectively satisfies customer requirements. The BSI recognised this reality early on, establishing a QM system as early as 2005, continuously developing it ever since. The German accreditation body DAkkS has accredited the BSI’s product certification for its Common Criteria area and other technical guidelines according to DIN ISO/IEC 17065:2013.

Optimising processes and systems are part of the daily thinking and actions of every employee. It is the only way to establish an effective, active, real-time QM system that supports continuous process optimisation.

Customer requirements also play a critical role in a thorough QM process. Development potential is absorbed not only internally, but externally as well, with various perspectives enabling a more comprehensive outlook.

CAPTURING CUSTOMER FEEDBACK
This way of thinking shapes our daily work at the BSI as well. Customer requirements play an important role in consciously implemented quality management, and the BSI developed an online survey to record customer feedback.

On this basis, regular customer satisfaction surveys are carried out and the findings analysed. Surveys take place after the completion of each certification and recognition procedure. Besides general questions on procedure handling, the experience gained in cooperation as part of
A total of 80 initial customer satisfaction surveys were sent out in the second quarter of 2018. The response rate was a respectable 34 percent.

Across all questions and evaluations, customers awarded an average score of 1.9 (according to the school grading system of 1 (best) to 6). The applicants were clearly very satisfied with BSI procedures. Customers were particularly impressed by the BSI staff’s professional competence and friendliness. Improvement potential was identified above all in “meeting deadlines, order processing and employee availability.” These results have been incorporated into the continuous improvement process to optimise processes. Evaluating future feedback will show whether the effort has led to the goal of continued quality improvement.

**SATISFIED CUSTOMERS**

A total of 80 initial customer satisfaction surveys were sent out in the second quarter of 2018. The response rate was a respectable 34 percent. Across all questions and evaluations, customers awarded an average score of 1.9 (according to the school grading system of 1 (best) to 6). The applicants were clearly very satisfied with BSI procedures. Customers were particularly impressed by the BSI staff’s professional competence and friendliness. Improvement potential was identified above all in “meeting deadlines, order processing and employee availability.” These results have been incorporated into the continuous improvement process to optimise processes. Evaluating future feedback will show whether the effort has led to the goal of continued quality improvement.

We would like to personally thank all those who contributed their feedback and suggestions for improvement as part of the customer satisfaction survey. We would also like to encourage all other customers participating in the certification and recognition process to take part in future surveys. Furthermore, everyone is welcome to send feedback and suggestions for improvement to “qmb@bsi.bund.de” at any time. Help us improve our quality for you.

**Your QM-team**
A Day at the BSI

IT security is diverse – and so are the tasks in the more than 100 departments at the BSI. Our colleagues Veronika Busch from the Section “Evaluation, Analysis and Monitoring of Secure Mobile Solutions” and Holger Schildt from the Section “IT-Grundschutz” demonstrate how information security can be designed in concrete terms.

Veronika Busch has been employed at the BSI since 2017. In addition to training as an IT specialist, she has completed two distance learning courses in Business Information Systems and IT Security. On weekends and in her free time, she pursue hobbies such as playing the piano, handicrafts and reading.

Holger Schildt began his career at the BSI as an intern in 2003 and was hired as a specialist advisor in 2005. Since May 2017, he has headed the BSI’s IT-Grundschutz section. In his spare time, Holger Schildt plays golf, enjoys the outdoors and jogs on the Rhine.

7:00 a.m.
Today is IT-Grundschutz Day in Berlin. About four times a year, we organise this event with several cooperation partners to present our professional work in the field of IT-Grundschutz and to exchange information with users from government and business. There is a final briefing with my team during breakfast at the hotel before we drive to the lecture venue.

10:00 a.m.
Joint greeting and opening of the day with the Managing Director of the cooperation partner. IT-Grundschutz has been in existence since 1994 and one of my colleagues presents how we have fundamentally modernised it. This is followed by a presentation by a BSI colleague on a current publication in the field of IT-Grundschutz. He explains how our “existing users” can migrate effectively and efficiently to modernised IT-Grundschutz. We then hear a very interesting presentation from an IT-Grundschutz user.

7:30 a.m.
My working day starts with a short breakfast while I start up my computer. The day before, details on some highly rated vulnerabilities were published.

My task is now to do research to gain an overview of the extent of the affected devices and to write a report on the effects of the vulnerability.

10:30 a.m.
After doing my research, it can be assumed that so-called “app-wrapping” is affected, which is supposed to protect a device’s integrity. I will now use a sample program to check the real effects of these vulnerabilities.
I attend mid-day sessions to inform colleagues of new publications and to inform them what the Section is currently analysing.

12:50 p.m.

I meet some colleagues for lunch and coffee.

12:45 p.m.

90-minute lunch break for all participants, speakers and organisers. During lunch, my staff and I take the opportunity to exchange current news and suggestions about IT-Grundschutz with users.

11:45 a.m.

App-wrapping is very important to prevent a device from being changed. I therefore examine it on a test laptop and a test mobile device. I load an application “secured” by app-wrapping onto the test device and compare its structure with the otherwise standard app structure. Then I check whether this app can be extended by malicious content.

I create a malicious code (a so-called “backdoor”) using a tool for penetration testing and add it to the app. I then extend the app’s notifications as necessary. I pack and sign the app and then install it on a mobile device.

I record all steps exactly so they are comprehensibly documented for my colleagues.

2:30 p.m.

In the next step, I will check to what extent the modified app can bypass the built-in integrity check. For today, however, I will share my findings with my colleagues and call it a day.

4:45 p.m.

I meet some colleagues for lunch and coffee.

2:15 p.m.

Two users explain in their lectures how our ideas can be put into practice.

In breaks between presentations, I have the opportunity to exchange ideas with some of the approximately 200 listeners.

Afterwards, I take over the last slot and present an outlook on planned projects, set goals, changes and dates.

4:30 p.m.

After a short debriefing with the cooperation partner, my colleagues and I go to the airport. After reviewing the day, I fly home in the evening with a sandwich and water from on-board catering.

2:45 p.m.

EVALUATION, ANALYSIS AND MONITORING OF SECURE MOBILE SOLUTIONS

The section focuses on evaluating the security of mobile solutions such as smartphones and tablets. Through targeted analysis and close communication with developers and testing laboratories, mobile solutions and their security can be evaluated and approved. Specifications and requirements for secure mobile communication are created and integrated through the process.

IT-GRUNDSCHUTZ

IT-Grundschutz is regarded as a benchmark in information security. The IT-Grundschutz methodology developed by the BSI makes it possible to identify and implement necessary security measures through a systematic approach – both in government and in companies of all sizes. Fundamentally modernised in 2017, IT-Grundschutz has been part of a sound professional debate on information security for more than 20 years.
Here’s to a Good Partnership

By Fabienne Tegeler, Section National Liaison Office, and Stefanie Euler, Section IT Security Consulting for Public Authorities

Designing cyber security in the digital age can be successfully achieved jointly by the federal and state governments. For this reason, the BSI consistently takes a cooperative approach, offering support to the federal states and taking the necessary steps to expand cooperation at various levels and achieve synergy effects.

The BSI and the Federal States

The cooperation’s overarching goal is to create a uniform IT security level in the Federal Republic of Germany. This goal is becoming increasingly important, especially in view of the ongoing digitalisation of government and the increasing connectivity of IT structures. Over the past two years, the federal and state governments have intensified their cooperation and driven cyber security forward, by developing a "Concept for the future coordination of IT security measures between federal and state governments, taking into account the role of the BSI” and developing guidelines for future cooperation.

BSI CONTACT ON SITE

The establishment of the National Liaison Office at the BSI deepens cooperation with the federal states. Permanent contacts with the federal states facilitate a close and regular exchange of information at state and municipal level. Since 2017, the BSI has been sending liaison officers to Wiesbaden and Berlin for this purpose. Since 2018, the western region is also being supported by the National Liaison Office from the BSI in Bonn. Further liaison offices were added in Stuttgart and Hamburg in early 2019.

In Berlin, the BSI has moved into its own premises for the first time for its liaison office at the centrally located Hausvogteiplatz in Berlin Mitte. This increases the BSI’s visibility in Berlin and will enable an exchange with politics, government, science and industry to obtain relevant information on cybersecurity issues.

FURTHER DEVELOPMENT OF COOPERATION AGREEMENTS

As the national competence centre for cybersecurity, the BSI supports the federal states as a central service provider in increasing cyber security. The aim is to make the BSI’s expertise available to the federal states at several interfaces. The cooperation is individually substantiated and fixed in cooperation agreements. The first cooperation agreements were signed in late 2017, followed by further agreements in 2018. Further agreements are in preparation for 2019.

ADMINISTRATIVE AGREEMENT – WHAT IS THIS?

Administrative arrangements and agreements under public law are similar in substance. They are to be distinguished from charter and constitutional treaties which are to be assigned to government activity. Administrative agreements are essentially only effective in the internal relationship between the parties involved and are binding between them until they are amended or cancelled. They therefore do not normally establish any direct rights and obligations in the external relationship for third parties. An indirect external effect is only possible via Article 3.1 of the Basic Law in conjunction with the principle of self-obligation of the administration.

Administrative agreements are no longer covered by the scope of the Administrative Procedure Act because of their quasi-normal character and their lack of legally binding external effect for and against third parties.
Die BSI-Angebote für die Länder

Partner cities with new BSI liaison offices

BSI SOLUTIONS FOR FEDERAL STATES

Due to the federal states' great demand for BSI products and services, non-binding cooperation agreements can only meet the supply and demand of services to a limited extent. In order to better plan resources (budget funds and personnel) on both sides, the cooperation between the BSI and the states will in the future be further developed via legally binding administrative agreements. The administrative agreement specifies the areas of cooperation in the cooperation agreement.

In this way, binding force is created for both sides and services to be provided by the state itself for subsidiarity reasons are clearly defined, as are which of the BSI's products and services that have proven their value at the federal level are to be used. The conclusion of administrative agreements will also promote synergies and strengthen the alliance between the federal and state governments against cyber threats.

The administrative agreements are based on a target audience-specific product catalogue initially comprising around 40 products and services from the various categories of the BSI portfolio for the states. In order to be able to use services beyond this, however, the corresponding legal bases still have to be adopted and business models developed at the state and federal levels.

When developing a framework for administrative agreements, the BSI closely coordinates with the Federal Ministry of the Interior and develops a suitable billing and retrieval procedure.

For more information see https://www.bsi.bund.de/BSI-vor-Ort
Data centres (DCs) must be protected. The choice of location needs to be considered carefully, the costs for construction and operation are very high, the design requires numerous strategic investments and risk decisions and the security aspects play a decisive role. Reliability, particularly availability, is a central requirement that a data centre must meet.

ACHIEVING RELIABILITY

The reliability aspects relevant to a data centre are described by numerous frameworks (e.g. ITIL v3, COBIT 5, ISO 27001, IT-Grundschutz, HV-Kompendium, Technical Standards and Guidelines). The term describes the expectation that an IT service – verifiable and comprehensible in advance – fulfils the required functions. Unfortunately, the ideal ideas of the first planning steps and the later reality of a data centre in operation are not congruent. In order to determine the actual reliability of an IT service or data centre, certain types of tools are needed.

One such tool is the HV benchmark (HVB). This makes it possible to determine the reliability of an IT service with relatively little effort and thus contribute to a strategic evaluation of the data centre. The HV benchmark was developed by the BSI in recent years in order to be able to carry out security analyses at computer centres. A version reduced to the direct IT security aspects, the HV benchmark compact (HVB-k), is now publicly available. The full version of the HVB is to be published shortly.

THE HV BENCHMARK CONCEPT

From the large number of possible aspects, 96 were selected for HVB which are of particular relevance for the assessment of reliability – so-called “indicators.” It is assumed that a computer centre operator or an IT service provider who has paid adequate attention to the particularly relevant aspects (indicators) has also dealt with all relevant aspects of an IT service to a comparable extent and with comparable care. This includes the systematic implementation of the above-mentioned best practices and frameworks.

WHAT TARGET AUDIENCES ARE BEING ADDRESSED?

The target audiences to be addressed by the HVB include, in particular, computer centre operators wishing, for example, to carry out a self-assessment or present their performance to customers. This work also addresses IT users looking for a suitable data centre operator / IT service provider and wanting to assess this provider from their own perspective.

METHODOLOGY AND IMPLEMENTATION

The central feature of the HVB is the use of a metric based on maturity models. It differentiates six levels from 0 to 5. The indicators considered in the HVB are assigned to three domains:

- Management.
- IT controlling.
- Technical implementation.
Within these three domains, a total of 14 sub-domains have been formed, to which one or more indicators are assigned (see figure).

The HVB methodology is essentially based on applying each indicator individually to the data centre and determining the level reached (0 to 5). Each level of an indicator is backed by one or more closed question(s). They must be answered with “Yes” or “No.” If the wording of a question is not fulfilled, but is implemented mutatis mutandis in the institution by a measure of equal or higher value, the requirement underlying the question shall be deemed to have been fulfilled. The level up to and including which all requirements of the client have been fulfilled. The level up to and including which all underlying questions could be answered with “Yes” is the level reached.

In further steps, results can be further condensed within the domains and sub-domains. Following the minimum principle, the domain or sub-domain assumes the value of its lowest indicator. The maturity / potential levels achieved can be well illustrated in spider diagrams, as they range from 0 to 5.

**EXAMPLE: APPLICATION OF THE HVB-K IN DATA CENTRES OF THE FEDERAL GOVERNMENT**

On the basis of a mandate from the Budget Committee of the German Bundestag, the BSI has for some time been investigating the security features of the Federal Government’s data centres with the help of the HV benchmark compact. The HVB-k considers only 34 of the original 96 indicators. The HVB-k is thus limited to those indicators that represent the “core” of IT security.

The HVB-k has now been used in around 100 federal data centres. The results are plausible and provide a good basis for further improving the reliability of the Federal Government’s data centres. Not least for this reason, the Budget Committee has annually renewed the investigation mandate and even expanded areas.
Artificial Intelligence (AI) is a generic term that refers to methods aimed at automating decision processes that traditionally require the use of human intelligence. As a research area, AI interacts closely with a large number of application areas, other sub-disciplines of computer science and more distant fields such as neurobiology.

All systems technically feasible today are considered so-called weak Artificial Intelligence. In contrast to strong AI (general Artificial Intelligence), no attempt is made to equip a machine with general intelligence comparable to human capabilities. Instead, a problem solving ability is implemented in limited contexts: For example, the system may play chess, make medical diagnoses or translate texts, but will have no (or very unreliable) capabilities outside its field of application.

Today’s AI systems usually use machine learning techniques as a key ingredient, for example through neural networks (see grey Box), deep learning, decision trees, cluster algorithms or support vector machines.

**AI-Based Techniques at the BSI**

At the BSI, the use of machine learning methods in various areas of IT security is being tested or evaluated or corresponding projects are being planned and prepared.

This concerns

- anomaly and attack detection in communications networks,
- automatic processing of natural language information for the creation of situation reports,
- the extent to which AI-based authentication procedures may be circumventable in the context of sovereign documents and
- the topic of explainable AI.

In addition, the section Evaluation of Cryptographic Mechanisms and Research Coordination is looking at the possibilities AI offers in cryptographic applications. In the future, AI methods that support emission security evaluations will also be studied.

**AI in the Evaluation of Cryptographic Systems**

Modern cryptographic algorithms are very secure against mathematical cryptanalysis. But they have to be implemented physically.

Side channel attacks aim at recovering the secret key by analysing the physical properties of the implementation (e.g. power consumption) during operation. They have played an important role for almost two decades, i.e. in the certification of smart cards. It is therefore indispensable to

Artificial Intelligence methods have revolutionised many computer applications in recent years. Well-known examples include automatic text translations, image and speech recognition systems and autonomous vehicles. Artificial Intelligence has also found its way into IT security. In its coalition agreement, the German government stressed the importance of Artificial Intelligence and presented a national AI strategy approved by the cabinet at the Digital Summit in December 2018. This emphasises the importance of the topic in the political arena as well.
Neural networks can be visualised by their connection graphs (see graphic). The data to be processed (e.g. measured values) is entered into the input layer (green neurons) and passed to the output layer (yellow neurons) via hidden layers (blue neurons). The initial values of all arrows entering a neuron multiplied by the weights (the numbers above the arrows) equal the input value for this neuron. The neurons calculate their output value by using a so-called activation function.

The weights are initially chosen randomly and then modified step by step so that the network predicts the training data well.

The weights later represent the “knowledge” of the network in live operation. In real applications, neural networks often consist of hundreds of thousands or even millions of neurons and a multitude of hidden layers. Still, non-trivial research results are occasionally achieved with relatively small neural networks.

know the best attacks. Scientific studies have shown that AI can support side channel analysis. For this reason, the BSI has also examined this topic with regard to approval and certification procedures.

As part of the CHES (the Conference on Cryptographic Hardware and Embedded Systems), the world’s most renowned hardware-related crypto conference, a side channel analysis competition was held in 2018. The authors of this article took part in two sub-disciplines and won both. The task was to determine the AES keys used from the power profiles of protected Advanced Encryption Standard (AES) implementations on microcontrollers. A combination of machine learning (neural network) and a traditional approach led to success. In another context, it was shown that neural networks (here: deep learning) can be used as a new supporting tool in the mathematical cryptanalysis of a block cipher as a new tool (see further information below).

ESTABLISHING OF AN AI COMPETENCE CENTRE AT THE BSI
At the end of 2017, the division Cryptotechnology and IT Management for Increased Security Requirements formulated the strategic goal of establishing a competence centre for AI and ML at the BSI in order to coordinate AI activities and take account of the increased importance of AI.

By arranging bilateral meetings with all interested parties within the BSI and by establishing a Machine Learning Project Group, a first common framework was created for AI-related activities at the BSI. In 2018, the series of events “Expert Workshop Machine Learning” was initiated in order to discuss current and future challenges in IT security with representatives from the scientific community. In addition, the visibility of the BSI was increased through public talks and participation in the platform Lernende Systeme. The BSI is also in regular contact regarding AI-related topics with international partner authorities.

In 2019, the new organisational structure of the BSI will further advance the establishment of the competence centre, now in a separate organisational unit. Internal and external AI activities will be coordinated there, and contacts to science and industry will be cultivated. Socio-political and ethical aspects will also play a central role.

OUTLOOK
Artificial Intelligence has already reached IT security and the areas of application will certainly expand in the future. The BSI will critically examine which applications are particularly well suited and where little or no improvements can be expected. Important topics for the future include, for example, explainable AI, dealing with incorrect decisions of AI systems and attacks on AI systems. The BSI will continue to build up expertise and help shape its further development.
Joining Forces to Ensure Secure Information Technology

ViSiT Attracts Many Participants from the German-speaking Regions
Cyber attacks know no borders. This is precisely why information security is an international concern that benefits from intensive cross-border cooperation. ViSIT, which took place as part of the it-sa security trade fair for the first time in 2018, brought together more than a hundred decision-makers and experts from public administration in Austria, Switzerland, Luxembourg and Germany.

The main focus of the international symposium held at the Nuremberg Exhibition Centre was on the state of digitalisation in public authorities. Public institutions do not want to and cannot afford to evade ongoing digitalisation. For them, too, it is a matter of making the best possible use of opportunities and mastering the respective challenges that arise.

The international symposium ViSIT is jointly organised every two years by the Austrian Centre for Secure Information Technology – Austria (A-SIT), the Swiss Federal IT Governance Body (ISB), Agence nationale de la sécurité des systèmes d’information Luxembourg (ANSSI.lu) and the Federal Office for Information Security (BSI). Its goal is to provide a platform for employees of the federal administration to obtain information and engage in exchanges on interesting security-related legal frameworks, projects, measures, implementations and experiences.
As the national cyber security authority, the BSI works in constant exchange with international partners on many levels. The BSI and its partners perform their tasks in the continuous transition of technologies and threats in very diverse fields. The European Union Agency for Network and Information Security (ENISA) has been working for many years to improve cyber security in Europe. With the “Cybersecurity Act,” the agency has been renamed the “European Union Agency for Cyber Security” and is at the crossroad of substantial changes.
CONNECTING THE DOTS

Due to the cross-border nature of cyber security, international exchange is an important component of the BSI’s role as the national cyber security authority. Besides its many contacts at bilateral and multilateral level, this increasingly includes close cooperation with EU institutions and agencies.

ENISA is a special partner in this context. As an EU agency with the task of “ensuring the necessary high level of network and information security in the EU,” ENISA has been active in the following areas since its foundation in 2004:

- Providing expertise in the continuously evolving digital sector,
- Supporting EU member states and institutions in developing and implementing EU regulations and policies,
- Capacity building for EU member states and institutions to increase cyber security in Europe,
- Promoting and maintaining EU-wide cooperation between EU member states, institutions, the private sector and other actors in the field of Network and Information Security (NIS).

ENISA is active in these areas in many ways – from EU-wide cyber security exercises to CERT cooperation, advice and analysis. However, the digital field of activity is characterised by a fast pace, the latest technical developments and a high threat level. Against this backdrop, the agenda of the European institutions and the role of ENISA are also changing.

IMPORTANT STEPS TOWARDS A DIGITAL EUROPE

At EU level, digitalisation and cyber security have increasingly become a top priority over the last decade. An important step in this context was the so-called “NIS Directive,” which came into force in August 2016 and whose implementation deadline in the member states passed on 10 May 2018. Germany fulfilled this obligation well in advance by laying the foundations in the IT Security Act and the Act on the Implementation of the NIS Directive, which passed on 23 June 2017.

For ENISA, the NIS Directive meant increased responsibilities. For example, it supports the new committees created as a result of the NIS Directive, namely the CSIRTs network of national Computer Security Incident Response Teams (CSIRT) for the operational exchange of information and the Cooperation Group at policy level.

Overall, the EU strategy focus “Digital Single Market” is experiencing significant growth under the new Multiannual Financial Framework of the European Union (2021-2027) and will in the future have additional funding opportunities through the “Digital Europe” programme with 9.2 billion euros – besides existing funding programmes.

European Commission President Jean-Claude Juncker, in his speech on the state of the Union in September 2018, called on the EU, as the world’s largest single market, to set standards in the digital sector in order to protect the values, rights and individuality of EU citizens. A cornerstone of these developments is the “Cybersecurity Act,” a regulation on cybersecurity published as a draft in September 2017 and whose negotiation was politically concluded in December 2018.

ENISA AND THE CYBERSECURITY ACT

Core elements of the “Cybersecurity Act” are a new permanent mandate for ENISA and the introduction of a common European cyber security certification framework. Both core elements go hand in hand. The Cybersecurity Act will introduce a framework for EU-wide cyber security certification. This will be accompanied by new tasks for ENISA, which in the future will coordinate the development of certification schemes and provide corresponding information management by maintaining an EU cyber security certification website. ENISA is also dedicated to supporting the new committees created by the Act, which are to advise on the development of certification schemes.

ENISA is also to be given an official supporting role in operational cooperation between member states and the EU, including the development of an EU-wide cooperative response to large scale cyber incidents and IT crises (the so-called “Blueprint”). Its new range of tasks is also reflected in ENISA’s increased budget, which is expected to nearly double, as well as in its staffing levels, which are expected to increase significantly in the coming years.
Regardless of whether it’s a mobile phone, cryptographic equipment or display device – hardware manipulations that give an attacker access to confidential information are conceivable with many electronic devices. X-ray technology can help detect these manipulations or at least make this much more difficult for the attacker.

THE THREAT SCENARIO
With hardware manipulations, attackers can intervene in various ways in the function of an IT device. Essentially, the following attack options can be distinguished:

- Installation of additional components: For example, the installation of a radio module in a keyboard can cause all keystrokes to be transmitted unnoticed by the user.
- Changes to the circuit or structure: For example, by removing parts of the electromagnetic shielding inside a display device, the image content may be radiated and received by the attacker.
- Manipulation by replacing chips: This involves installing new chips with a modified or extended functionality.
PREVENTION OF MANIPULATIONS

Examining suspicious devices more closely in an X-ray system can detect such attempts of manipulations. Particularly devices exposed to a higher risk of manipulation can be examined several times during their period of use. Ideally the first examination should take place directly after production on the basis of a trustworthy configuration. This will be used to generate reference images. The results of subsequent examinations can then be compared with the reference images so that changes can be clearly detected.

Changes in soldered components can often be easily detected by X-ray imaging. If an attacker tries to manipulate the assembly shown in Figure 1 on the top, for instance, by replacing the chip, the impact of this process can be clearly seen on the two X-ray images. During the soldering process, a random pattern of flux, solder and air forms beneath the components that cannot be reproduced. Vias fill more or less with solder and appear as brighter or darker dots.

2D EXAMINATION WITHOUT REFERENCE IMAGES

Reference images of devices suspected of being manipulated are not always available, however. In these cases, an attempt can be made to obtain an identical model to compare the two devices. Since manufacturers often change the interior of their devices, e.g. depending on component availability, direct image comparison is often difficult. The only option is to search manually for obvious anomalies. A piece of cable that is obviously laid manually, as shown in Figure 2, definitely demands closer inspection.

3D EXAMINATION

A further examination option is to produce a three-dimensional scan. During a complete rotation of the object under examination, several thousand fluoroscopies are made. From these, a 3D model is then created by a computational algorithm (computer tomography).

Different views can be generated from this model for further analysis, and virtual section planes can be created. In Figure 3, two sides of the housing were initially removed. This allows for a detailed view of the interior of the device. Subsequently, the horizontal slicing plane was moved downwards. In this way, the other layers of components could be displayed and examined.

AVAILABLE X-RAY TECHNOLOGY

The BSI operates an X-ray facility which is capable of several kinds of non-destructive examinations. Depending on the application, both simple 2D fluoroscopies and complete 3D scans of the objects can be performed. These X-ray examinations offer a fast, usually non-destructive way to gain insights into the inner workings of an IT device. Manipulation detection is possible quickly and reliably, especially if reference images of a trustworthy configuration were taken before the device was used for the first time.
An IT-Grundschutz profile is a practicable solution, especially for small and medium-sized enterprises (SMEs), to increase information security within the company at a reasonable cost in terms of personnel and financial resources. Since the beginning of 2018, the BSI has been supporting interested federations and trade associations from various industries on developing such model security concepts with a workshop concept as part of the Alliance for Cyber Security (ACS) and IT-Grundschutz. After just three interactive events, an initial IT-Grundschutz profile can be created that is individually attuned to the respective requirements.

The digital transformation is constantly evolving in medium-sized businesses. Although SMEs recognise the threat posed by cyber risks and the need for appropriate protective measures, there is often a lack of structured creation and implementation of information security concepts and processes. For the implementation of an Information Security Management System (ISMS), the range of questions to be clarified extends from risk analysis and the secure storage of confidential data to raising employee awareness of current cyber threats. The BSI’s IT-Grundschutz offers a proven, holistic methodology that covers all these issues and supports SMEs in raising the level of information security. Industry-specific IT-Grundschutz profiles are a practical working aid, particularly for smaller companies.

WORKSHOP CONCEPT: IT-GRUNDSCHUTZ PROFILES MADE EASY

In an IT-Grundschutz profile, the individual steps of a security process are bundled and documented for a defined area of application. These sample security concepts are particularly well suited for industries, sectors or other associations of institutions with similar conditions and can be created by user groups rather easily. The intensive exchange between participants with different perspectives on the respective requirements usually leads to a good result.

Since the beginning of 2018, the BSI has been supporting interested federations and trade associations from various industries with a workshop concept as part of the ACS,
which enables user groups to develop an IT-Grundschutz profile with manageable effort. The interactive creation process offers a variety of advantages to all participants, from the expansion of industry and IT security expertise to information on the implementation of IT-Grundschutz and networking with the participants for a sustainable and in-depth exchange of experience within the framework of the (newly) established network.

ACHIEVING A LOT TOGETHER WITH A MANAGEABLE DEGREE OF EFFORT
Practical experience has shown that a “light version” of an IT-Grundschutz profile can be created by attending only three five-hour workshops. In addition to a generalised reference architecture with a corresponding determination of the need for protection, it includes a selection of suitable IT-Grundschutz modules as well as information for further risk analysis to be carried out individually, if necessary. This version is now ready for publication so that other companies in the same industry can also benefit from the security considerations and adapt them to their own individual needs.

“MAPS” FOR DEMAND-ORIENTED PROFILE USE
The “maps” produced during the second workshop are a key result of the production process. In graphic form, they offer virtually everything at a glance and open the door to the individual information security process. They can serve as a basis for company decisions as well as an “implementation roadmap” for IT experts. The “light version” of the IT-Grundschutz profile provides a practical basis for implementation. In the further course of the creation process, the parties can decide to enrich the IT-Grundschutz profile with more detailed recommendations on the requirements and implementation instructions.

The BSI invites companies, associations, chambers and authorities to create industry-specific IT-Grundschutz profiles and offers support with the workshop concept as part of the Alliance for Cyber Security (www.allianz-fuer-cybersicherheit.de).

“I accepted the invitation to the first event because I was hoping to receive more information on the implementation of ‘Maritime Cyber Risk Management’ at a shipping company. The event offered the opportunity to work together with other shipping companies on a ‘standard’ that could serve as the basis for a ‘Maritime Cyber Risk Management System’ in the future. I am completely convinced of this approach and I’m very grateful to the process initiator, the Association of Hanseatic Marine Underwriters, and the BSI for establishing a platform for this purpose. The IT-Grundschutz profiles for shore and ship operations will serve as a very good basis for implementing IT security and data protection for a shipping company in the future.”

Kersten Gevers, Managing Director of afEfa Verwaltungsgesellschaft mbH

Previously published IT-Grundschutz profiles from the trades, for shipping companies etc. can be found at https://www.bsi.bund.de/profile
Made-to-measure Security

Increasing Cyber Security in the German Craft Sector

By Dr. Stefan Wunderlich, Section Cyber Security for the Private Sector

Small and medium-sized companies are increasingly becoming targets for cyber attacks – often causing considerable economic damage. As part of the cooperation with the German Confederation of Skilled Crafts (ZDH), the Alliance for Cyber Security supports crafts businesses in increasing their resilience against current cyber threats.

Digitalisation has caught on in the German craft trades for quite some time. IT-based processes are becoming more and more important in the office and in the workshop, whether for customer acquisition, preparing offers, executing orders, invoicing or, ever more frequently, to control tools and machines. In order to ensure the continuity of operational processes and to benefit from the opportunities offered by digitalisation in the long term, the trades need to actively deal with the question of information security.

COOPERATION BETWEEN THE BSI AND THE ZDH – A SUCCESS MODEL

Against this backdrop, the German Confederation of Skilled Crafts (ZDH) and the BSI have agreed on a long-term cooperation. ZDH president Hans Peter Wollseifer and the President of the BSI, Arne Schönbohm, signed a letter of intent in October 2017. The goal is to raise awareness of IT security in craft businesses and support them in implementing preventive protective measures. The corresponding activities and offers such as events, online platforms, videos and information brochures are realised with great success under the umbrella of the Alliance for Cyber Security (ACS).

The ACS has hosted three Cyber Security Days specifically for craft associations and businesses. Besides providing information on the current threat situation, the focus was on developing recommendations for actions and solutions that are also suitable for smaller businesses. Under the slogan “Fit for Digitalisation,” the ACS together with the Digital Crafts Competence Centre visited several German cities to train people in the local chambers and associations.

A special highlight of the cooperation is the compilation of tailor-made IT-Grundschutz profiles for chambers of crafts and businesses. These can be used by organisations with similar conditions and requirements as templates for their own individual security concepts, saving time and money. The IT-Grundschutz profile for Chambers of Crafts was released to potential users in July 2018. A profile for crafts enterprises and the corresponding handbook for practical implementation can be found on the ACS website at www.allianz-fuer-cybersicherheit.de.

For further information see www.allianz-fuer-cybersicherheit.de
What opportunities does digitalisation offer for the German craft sector? The digital transformation opens up a wide range of possibilities for trades. Businesses can optimise the use of resources, improve work processes, develop new business models and tap into digital markets. Besides entrepreneurial creativity and a nationwide broadband, we also need good basic conditions for successful digital change.

How do you assess the awareness of cyber risks in the trade? The increasing uncertainty with regard to cyber security, in addition to a lack of resources and digital know-how, is a key reason why many potentials of digitalisation remain untapped and companies are putting digitalisation projects on hold. This is a finding of the latest ZDH study. However, as the networking of systems is increasing rapidly and the degree of digitalisation is rising constantly, craft enterprises are targeted more often by hackers, malware, phishing and other cyber attacks. This leads to anxiety among the owners. Cyber security is therefore becoming an essential prerequisite for successful digitalisation.

For you, what have been the highlights of the cooperation between the ZDH and the BSI so far? Our joining the Alliance for Cyber Security (ACS) was definitely an important milestone in our cooperation. As a member of the Advisory Board, the ZDH brings the craft perspective into the dialogue process and plans to help develop the range of services for small and medium-sized enterprises. As part of our cooperation, the ACS and the German Confederation of Skilled Crafts (KDH) have already implemented interesting information and dialogue formats. These include the Cyber Security Day for the crafts, the roadshow “Cyber Security – Fit for Digitalisation” and online offers at www.handwerkdigital.de. They make a decisive contribution to sensitising craft businesses to current developments, opportunities and challenges in the area of cyber security.

How can companies benefit from the offers of the BSI? It is really quite simple: by becoming a participant in the Alliance for Cyber Security. We regularly encourage our member companies to do so. The offer is free of charge and allows the participants to benefit from the ACS network of experts and the expertise of the BSI. They receive regular security warnings and news as well as guidance on implementing security measures in their own business.
Higher Security on the Internet for Citizens

BSI für Bürger Brings Digital Trends and IT Security Closer to Home

Whether it’s networked dolls listening in on children’s rooms or cyber criminals hacking passwords: every digital technology potentially also harbours IT security risks. BSI für Bürger informs consumers about current issues, explains them – and gives tips on how to use these technologies responsibly.

Toys with an integrated Internet, so-called Smart Toys, are currently conquering Germany’s children’s rooms. But what if the smart doll is also equipped with a microphone? Then the sweet toy quickly becomes a spy in the nursery – of course only if the parents don’t know that it has a microphone and how to switch it off.

BSI für Bürger picks up on the BSI’s very own subject in our everyday lives: IT security in the information society. It explains trends and technologies of digital life and supports citizens in their conscious use. It is about more than just information. Above all, BSI für Bürger offers practical tips on how to handle the risks.

SAFELY AND THOROUGHLY INFORMED VIA ALL CHANNELS
Online texts, newsletters and security alerts, videos and podcasts with BSI experts help keep interested parties up to date. The BSI is currently focusing on e-mail encryption and two-factor authentication for citizens.
Wherever people exchange texts, photos and videos about their private lives, cyber criminals are not far away either. Weak passwords are the perfect gateway for them, as recent months have once again shown. This is especially true with social media. Many platforms now offer two-factor authentication (2FA), an additional form of identification to the password. BSI für Bürger explains the possibilities of 2FA, in an expert video, for instance.

BSI für Bürger is also active as part of European initiatives. Ultimately, IT security doesn’t take place within national borders. The annual European Cyber Security Month (ECSM) calls for action on the issue of cyber security. The BSI was also the coordinating body of the ESCM in Germany in 2018. Interactive quiz formats that focus, among other topics, on the basics of IT security in one’s own home can be found on www.bsi-fuer-buerger.de, Facebook and Twitter to ensure that a toy remains a toy.

For further information see

https://www.bsi-fuer-buerger.de

http://www.facebook.com/bsi.fuer.buerger

Mit dem Bürger-CERT-Newsletter sicher informiert: https://www.bsi.bund.de/Buerger-CERT
EVENTS IN 2019

16th German IT Security Conference

21-23 May 2019 in Bonn-Bad Godesberg

Under the motto “IT security as a prerequisite for successful digitisation,” the BSI is organising the 16th German IT Security Conference in Bonn from 21 to 23 May 2019.

The keynote speeches will be held by the Federal Minister of the Interior, Horst Seehofer, the Federal Commissioner for Data Protection and Freedom of Information, Ulrich Kelber, and the Mayor of Bonn, Angelica Maria Kappel. Besides an international programme block on the subject of “Supply Chain Security in Digitalisation,” the German IT Security Conference will offer an overview of current topics, challenges and solutions in cyber security in Germany and internationally in around 50 expert lectures.

The conference, which the BSI organises every two years, is a fixed event in the calendar of events of the IT security industry. For three days, the participants discuss the status of national and international developments in IT security. The aim of the conference is to shed light on the topic of IT security from different perspectives, to present approaches to solutions and to further develop them. The selection of topics and lectures is traditionally decided on by an external programme advisory board consisting of twenty experts from the areas of IT and cyber security. An accompanying exhibition complements the presentation programme.

it-sa

08-10 October 2019 in Nuremberg

From 08 to 10 October 2019, the BSI will be represented with a booth and various lecture activities at it-sa in Nuremberg. The BSI, together with the Federal Association for Information Technology, Telecommunications and New Media (Bitkom e.V.), acts as the idealistic sponsor.

it-sa is the only IT security trade fair in the German-speaking world and one of the most important in the world. Whether it’s cloud computing, IT forensics, data backup or hosting: the trade fair is a unique platform for IT security officers, developers and providers of products and services relating to IT security.

For more information see https://www.bsi.bund.de/Veranstaltungen
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 issues by mail following the Hannover Messe in April and it-sa in October 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

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 200363, 53133 Bonn, Germany, is responsible for processing your aforementioned personal data. The information 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 before revocation. For more information on how we process your personal data and what rights you are entitled to, please refer to the “Data Protection Information” attached for ordering BSI publications.

Simply send in the form by fax or email:
Fax: 0228 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 at bsi-magazin@bsi.bund.de.

Follow the BSI on Facebook and Twitter!
www.facebook.com/bsi.fuer.buerger   |   twitter.com/bsi_presse
For more information, checklists and tips on cyber security, see
Privacy Policy Regarding the Subscription to BSI Publications

Responsible handling of personal data is a high priority for the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI). We want you to know whenever we collect certain data and how we use it. We have taken numerous technical and organisational measures in order to ensure that the regulations on data protection are complied with, both by us and by our external service providers. In the course of further development and the implementation of new technologies, changes to this privacy policy may be necessary. We therefore recommend that you re-read this privacy policy from time to time. A current version can be requested at any time from the BSI or can be found in the next issue of the BSI Magazine.

1. RESPONSIBLE BODY
The responsible body for the processing of personal data within the meaning of the EU General Data Protection Regulation (GDPR) and other data protection provisions is the Federal Office for Information Security (BSI), Godesberger Allee 185-189, 53175 Bonn, bsi@bsi.bund.de, Phone: +49 (0)228 99 9582-0, Fax: +49 (0)228 9910 9582-0, www.bsi.bund.de.

2. BSI’S DATA PROTECTION OFFICER
BSI’s Data Protection Officer is Frau Elke Gräf, Federal Office for Information Security, Godesberger Allee 185 -189, 53175 Bonn, Phone: 0228 99 9582-5775, Fax: +49 228 9910 9582-5775, E-mail: datenschutzbeauftragte@bsi.bund.de.

3. GENERAL INFORMATION ON THE PROCESSING OF DATA
a) Purposes of Processing
Provided you have given your consent, the BSI or its appointed service provider uses, electronically stores and processes your personal data for the purpose of the distribution of BSI publications. All processing of personal data is based on the declaration of consent of the respective data subjects within the meaning of Art. 6 para. 1 lit. a), Art. 7 GDPR.

b) Recipients and Categories of Recipients of Personal Data
Personal data will be transferred to the following third parties: shipping service providers. Personal data will otherwise only be transferred to third parties (public authorities, companies, private individuals) insofar as the BSI is required to do so by law or court order or in the event of attacks on the Internet infrastructure for legal or criminal prosecution. No further disclosure to third parties will be made without the data subject’s consent.

c) Duration of Storage and Criteria for the Duration of Storage
Your personal data, which is used to deliver BSI publications, will only be processed for that purpose and as long as you have not cancelled your subscription or withdrawn your consent.

Any other inquiries to the BSI will be kept in paper or electronic form in accordance with the limitation requirements according to the Registry Directive applicable to the retention of records. The use of your data is solely for direct correspondence with you.

d) Rights of Data Subjects
In case the BSI processes your personal data, you as the data subject are entitled to the following rights in dealing with the BSI:

i. Right of Access
You have the right to obtain from the BSI confirmation as to whether or not personal data concerning you is being processed. Where that is the case, you can require the BSI to provide the following information:
• the purposes of the processing of personal data;
• the categories of personal data that are processed;
• the recipients or categories of recipient to whom the personal data about you has been or will be disclosed;
• the envisaged period for which the personal data will be stored, or, if specific information is not possible, the criteria used to determine that period;
• the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning you or to object to such processing;
• the right to lodge a complaint with a supervisory authority;
• where the personal data is not collected from the data subject, any available information as to its source;
• whether personal data concerning you is transferred to a third country or to an international organisation; in this event you have the right to be informed of the appropriate safeguards pursuant to Article 46 GDPR concerning the transfer;
• the existence of automated decision making, including profiling, referred to in Article 22(1) and (4) GDPR and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

ii. Right to Rectification
You have the right to rectification and/or completion against the BSI if the personal data processed that relates to you is incorrect or incomplete. The BSI will make the correction without undue delay.

iii. Right to Restriction of Processing
Under the following conditions, you have the right to obtain restriction of processing of personal data concerning you:
• if the accuracy of the personal data is contested by you, for a period enabling the BSI to verify the accuracy of the personal data;
• if the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead;
• if the BSI no longer needs the personal data for the purposes of the processing, but it is required by you for the establishment, exercise or defence of legal claims, or
• if you objected to processing pursuant to Article 21(1) GDPR pending the verification whether the legitimate grounds of the BSI override your grounds.

Where processing of your personal data has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject’s consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. If you have obtained restriction of processing pursuant to the preconditions above, you will be informed by the BSI before the restriction of processing is lifted.

iv. Right to Erasure
You have the right to obtain from the BSI the erasure of personal data concerning you without undue delay and the BSI has the obligation to erase this data without undue delay where one of the following grounds applies:
• the personal data concerning you is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
• you withdraw consent on which the processing is based according to Article 6(1a), or Article 9(2a) GDPR, and there are no other legal grounds for the processing;
• you object to the processing pursuant to Article 21(1) GDPR and there are no overriding legitimate grounds for the processing, or you object to the processing pursuant to Article 21(2) GDPR;
• the personal data concerning you has been unlawfully processed;
• the personal data concerning you has to be erased for compliance with a legal obligation in Union or Member State law to which the BSI is subject;
• the personal data concerning you has been collected in relation to the offer of information society services referred to in Article 8(1) GDPR.

If the BSI has made the personal data public and is obliged pursuant to Article 17 (1) GDPR to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers who are processing the personal data that you as the person affected have requested the erasure by such controllers of any links to, or copy or replication of, this personal data.
You do not have the right to erasure of the personal data concerning you to the extent that processing is necessary:
• for exercising the right of freedom of expression and information;
• for compliance with a legal obligation which requires processing by Union or Member State law to which the BSI is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the BSI;
• for reasons of public interest in the area of public health in accordance with Article 9(2h) and 9(2i), as well as Article 9(3) GDPR;
• for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) GDPR in so far as the right referred to in section a) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
• for the establishment, exercise or defence of legal claims.

v. Right to Data Portability
You have the right to receive the personal data concerning you which you have provided to the BSI, in a structured, commonly used and machine readable format. You also have the right to transmit this data to another controller without hindrance from the BSI to whom the personal data has been provided, where:
• the processing is based on consent pursuant to Article 6 (1) a) or Article 9 (2) a) GDPR or on a contract pursuant to Article 6 (1) b) GDPR; and
• the processing is carried out by automated means.

In exercising this right, you also have the right to have the personal data concerning you transmitted directly from one controller to another, where technically feasible. The rights and freedoms of other persons must not be adversely affected by this. The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the BSI.

e) Right to Withdrawal of Consent
You have the right to withdraw your consent given at any time. For this purpose, please send an email to bsi-magazin@bsi.bund.de. To unsubscribe to newsletters from the BSI, please use the link shown at the end of each newsletter. The withdrawal of consent will not affect the lawfulness of processing carried out on the basis of such consent before its withdrawal.

f) Right to Lodge a Complaint with the Supervisory Authority
Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement if you feel that the processing of personal data relating to you infringes the GDPR. The supervisory authority for the BSI is the Federal Commissioner for Data Protection and Freedom of Information (BfDI). The supervisory authority with which the complaint has been lodged will inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78 GDPR.

g) Necessity of Data Collection
The ordering of BSI publications as well as the provision of all information in this context is generally voluntary. We point out, however, that in case of incomplete information regarding your name and your contact details, delivery of these publications may not possible.
The BSI Magazine is published bi-annually. It is part of the Federal Office for Information Security’s public relations work. It is provided free of charge and is not intended for sale.