Federal Office
for Information Security

BSI Magazine 2017/02

Security in focus

Information Security as the Prerequisite for Digitalisation

CYBER SECURITY

The BSI in Operation on Site

THE BSI

Cyber Security in Digitalisation

IT SECURITY IN PRACTICE

Without Cooperation, You Won't Get Very Far

EDITORIAL

Everything from a Single Source

The massive cyber attacks of the recent past have shown that the major digitalisation projects in Germany and the use of the Internet of Things by our citizens are only a gain for us all if an appropriate security level can be ensured.

The IT Security Act, the KRITIS regulations, the regulations in the Telecommunications and NIS Implementation Act create a solid framework for higher IT security. They require numerous players to ensure an adequate level of security and report incidents. The focus of the BSI goes even beyond this, however. As the national cyber security agency, it is our job to shape information security in digitalisation. That is why we also approach those who are not directly subject to the above-mentioned regulations.

No company likes to admit that it has fallen victim to a cyber attack; no PC user gladly admits that ransomware irretrievably encrypted all of his data. They must trust the authority they turn to in such cases.

A representative survey conducted by the BSI recently showed that 87 per cent of respondents consider security on the Internet an important aspect, but less than half say they are familiar with this topic. Two-thirds say that security tests, security guidelines and clear liability provisions contribute to more security in cyber space.

Furthermore, a study published by DIVSI showed that four out of five respondents advocated the introduction of a security seal for trustworthy offers and services on the Internet. 85 per cent of Internet users in Germany agree that the government should deal more with Internet security, and 80 per cent said they were in favour of a central competent authority in Germany for all security-related tasks on the Internet.

“As the national cyber security agency, it is our job to shape information security in digitalisation.”

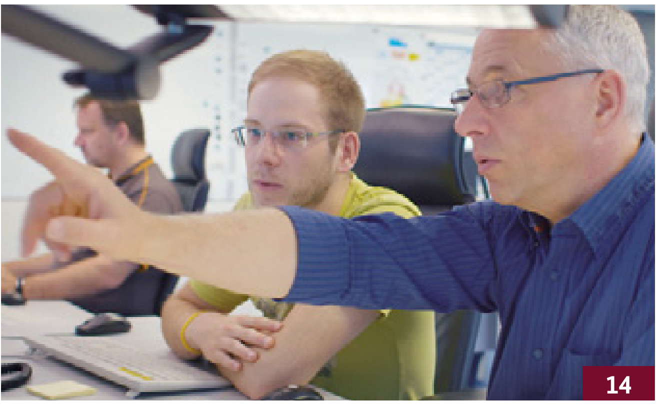
The BSI already is this central authority. In its current form, it has a unique selling point – its internal networking. Experts from the special field of information security work more closely and directly together at the BSI than anywhere else. This bundling and networking of cyber security expertise in one agency gives the BSI its high impact in Germany. For this reason, insights from operational cyber defence can be introduced to prevention, standardisation and certification without delay. Therefore, new findings from the basic work of cryptography are incorporated into the defence capabilities of the BSI. That is why this knowledge can be comprehensively prepared and communicated. For this reason, the BSI initiates the dialogue with the government, the business world and society and seeks to gain acceptance of cyber security issues.

You’ll find many of these exciting topics in our BSI Magazine. I hope you enjoy reading it!

Arne Schönbohm

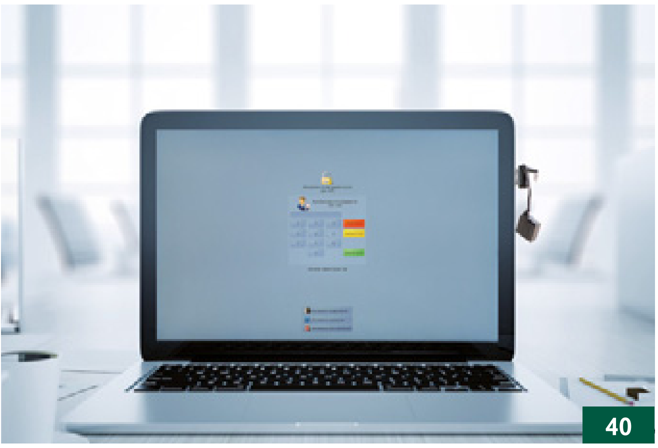
Arne Schönbohm,
President of the Federal Office for Information Security

8



14

38



40

52

TABLE OF CONTENTS

NEWS

BSI INTERNATIONAL

CYBER SECURITY

THE BSI

IT SECURITY IN PRACTICE

DIGITAL SOCIETY

NEWS

10 Years of UP KRITIS

"We are UP KRITIS!" – 10 Years of Comprehensive Protection of Critical Infrastructures

On the occasion of the 10th anniversary of the public-private partnership, a conference for critical infrastructure operators, authorities and associations was held in Berlin on 30 May 2017. Under the motto "We are UP KRITIS!" some 200 participants exchanged ideas on current challenges with the integral protection of critical infrastructures.

In order to prevent a failure of the critical services essential to the society, UP KRITIS pursues the all-hazard approach, which encompasses possible dangers from the physical as well as the cyber world. The aim of UP KRITIS is to ensure that the population is supplied with the essential goods and services of critical infrastructure such as energy, water, transport and food. The goal of the BSI and the operators of critical infrastructures is to continue to improve their protection in the future as well.

For more information see https://www.bsi.bund.de/UP-KRITIS

Final Event SuSi

Secure Digital Society

On 7 September 2017, the BSI presented the results of the project "Digital society: smart & secure" in the Kalkscheune in Berlin. The "impulses for a smart and secure digital society" were discussed with representatives of civil society, the business world, government and science.

You'll find more information on the project on page 58

ECSM

European Cyber Security Month 2017

This year, cyber security will once again be the focus in October. Under the aegis of the ENISA (European Agency for Network and Information Security), activities on cyber and IT security will be offered across Europe for EU citizens, organisations and companies for the fifth time. The aim is to sensitise people to these issues and raise awareness of cyber threats. The BSI is the national coordination centre for the ECSM in Germany and calls on organisations to participate by conducting their own activities on greater cyber security.

For more information see https://www.bsi.bund.de/ECSM

it-sa 2017

Even More International in New Halls

Larger and even more international – this year, the trade fair it-sa will occupy two halls. Around 580 exhibitors will present IT security solutions from the areas of hardware and software as well as research and services from 10 - 12 October at the Nuremberg Exhibition Centre. International community booths from France, Israel and the Czech Republic will enrich the exhibition offer. Those responsible for IT security and decision-makers can also look forward to four open forums with lectures and discussion sessions in the exhibition halls and the accompanying conference programme. This year, on 11 October the IT-Grundschutztag will be held under the umbrella of the it-sa congress and the five year anniversary of the cyber-security alliance.

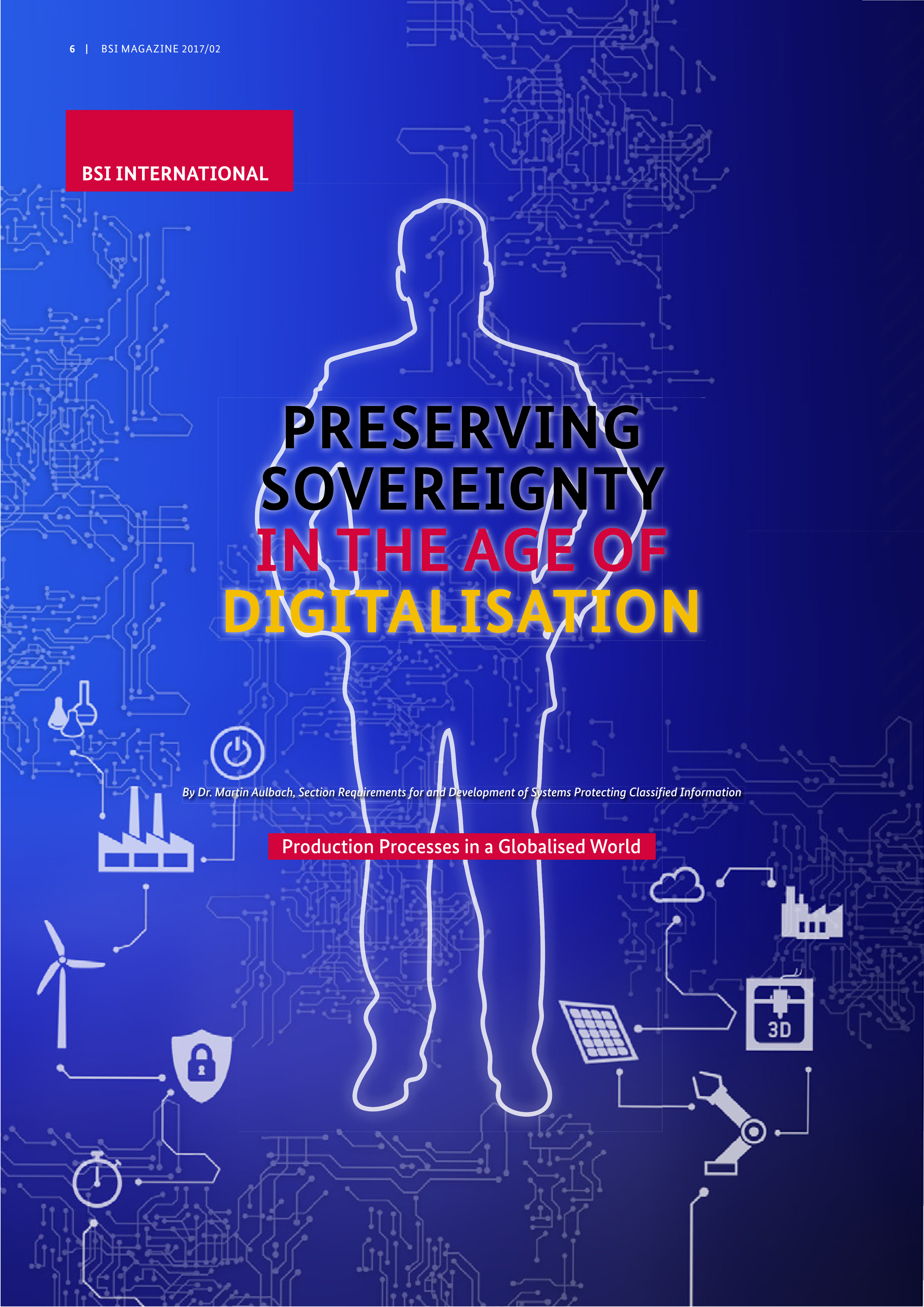
For more information see www.it-sa.de

Secure Pim iOS

The BSI Enables Secure Use of iPhones and iPads by the Government

The Federal Office for Information Security (BSI) already approved the solution SecurePIM Government SDS from the manufacturer Virtual Solution back in 2015 for use by the federal government. After continuation of the security evaluation with the aim of final approval, the BSI has adapted the usage and operating conditions based on the results thus far so that federal states, municipalities and companies can use iPhones and iPads with SecurePIM in the manner approved by the BSI for classified information in the area of critical infrastructures. Until now, the operation of SecurePIM was only possible inside the government network. Furthermore, it is also possible to use it in other networks in which classified data is stored, transmitted and processed.

BSI INTERNATIONAL



PRESERVING SOVEREIGNTY IN THE AGE OF DIGITALISATION

By Dr. Martin Aulbach, Section Requirements for and Development of Systems Protecting Classified Information

Production Processes in a Globalised World

Germany's ability to act and sovereignty must also be preserved in the age of digitalisation. This requires a guideline which is part of the Federal Government's Cyber Security Strategy. A competitive national IT industry that is bound to local law represents an important tool for this. Only then can the requirements for the IT security of processes and products be properly enforced.

In Germany, there are strict regulations for the storage and processing of personal data. In general, however, they cannot be applied and enforced if, for example, email services or cloud storage of companies based outside Germany are used. For example, Yahoo, a company that does business internationally, recently refused to provide the BSI with details regarding the theft of access data for one billion email accounts, although German citizens were also affected by this incident..

Most IT products or their components are no longer manufactured in Germany or the EU. Furthermore, increasing market consolidation can also be observed in the semiconductor industry. This reduces the choice of manufacturers of these components. But if you do not have complete control over the manufacturing process or the supply chain, manipulations of the finished IT system can no longer be ruled out. This is not an abstract threat scenario: Current media reports suggest that a factory-installed backdoor was found in the firmware developed by a Chinese advertising company in 700 million Android devices sold worldwide.

RELIABLE MANUFACTURING PROCESSES

Internationally operating companies whose registered office does not allow national law to be applied, IT products developed in other countries, supply chains around the world: All these are the logical consequences of globalised industrial production. They bring challenges for IT security. The BSI responds to these challenges by taking various measures. They are aimed at enabling and promoting trustworthy manufacturing processes. The BSI thus positions itself on a strategic level to use open source and free software.
IT security is strengthened by fully understanding and developing source codes even further.

The BSI acts as a user as well as a provider of free software. The products developed or sponsored by the BSI under free licenses include, for example, Gpg4win, OpenVAS and SINA (Secure Inter-Network Architecture). This Linux-based product family is used, among other purposes, for secure communication between the German embassies and the Federal Foreign Office. With SINA, secure storage, processing and transmission of officially classified information is possible up to secrecy level CONFIDENTIAL.

SELF-DEVELOPMENT AS AN ALTERNATIVE

If no free access to the source code or the exact structure of an IT product is possible, the BSI can convince itself of the correct functionality of the product through a cooperation agreement with the manufacturer. In addition, the BSI can also develop the IT products or subcomponents the Federal Government requires by itself. This is done by way of invitations to tender. Companies that are willing to meet the requirements of the BSI with regard to the greatest possible transparency of the development process can apply for this. This was the case in the original call for tenders for SINA in 1999, for example, when secunet Security Networks AG was awarded the contract.

If there is no alternative to the use of non-trustworthy subcomponents in an IT system for processing certified information, the risk can finally be reduced to an acceptable level by means of a suitable conception of the entire IT system. In this case, for example, the BSI's experts isolate the non-trustworthy components so strongly from the rest of the system that they cannot cause any damage. ■

Final inspection before the main conference

G20 – Counter Eavesdropping

Ensuring Confidentiality

Discussions on internationally relevant political topics, one-to-one meetings, and the struggle to find the right wording in negotiations determine the course of events at political conferences such as the G20 Summit in Hamburg in July 2017. Thanks to its technical expertise on preventing interception, the BSI ensured that all of this could take place in a confidential and sound-proof environment.

Family photo of the G20 heads of state and the invited G20 participants

Left photo: Measurements for abnormalities on the IT network using a special analyser

Right photo: BSI workplace for checking the high-frequency spectrum, also with regard to mobile communications and IMSI-Catchers, in the conference area

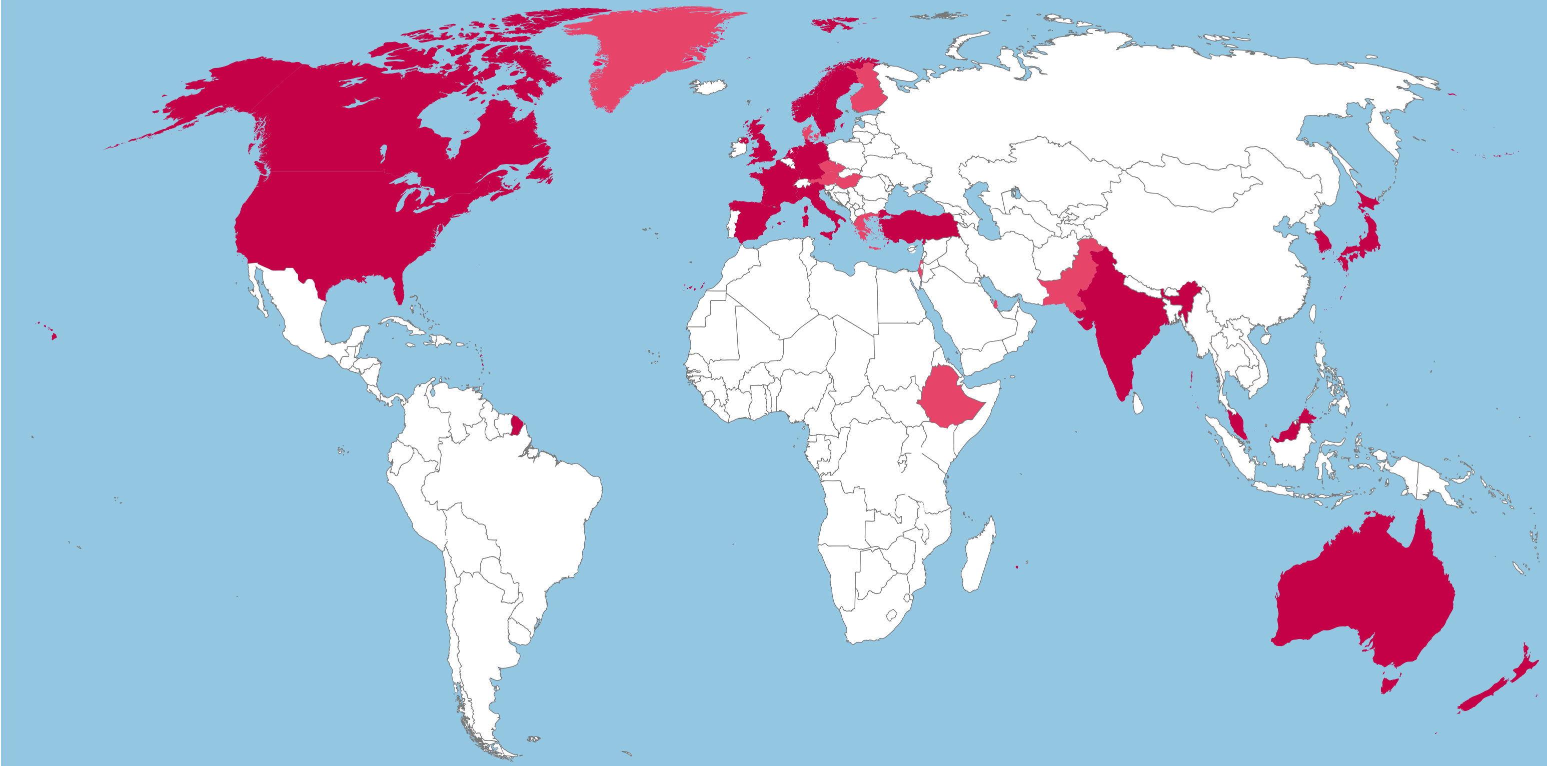
Left photo: broadcasting activities were monitored by BSI staff and analysed for abnormalities in the measuring vehicle

Right photo: Interpreters were asked to deposit their mobile phones outside the interpreting booths so that no confidential conversations could be recorded or transmitted to the outside world

GLOBALLY CERTIFIED

By Matthias Intemann, Head of Section Certification of Software and COTS Products

More than 25 Nations Work Together



THE COMMON CRITERIA – THE CCRA

■ **Certified nations**

Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, the Netherlands, New Zealand, Norway, United Kingdom, Singapore, Spain, South Korea, Sweden, Turkey, USA

■ **Acknowledging nations**

Austria, Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Israel, Pakistan, Qatar

The product certificates of the BSI according to the international standard Common Criteria are recognised worldwide and especially in Europe. This is based on the two Recognition Agreements Senior Officials Group Information Systems Security (SOG-IS) and Common Criteria Recognition Agreement (CCRA). The BSI actively contributes to both agreements in order to strengthen the value of the certificates and ensure that Germany's national interests are met.

CURRENT DEVELOPMENTS OF THE CCRA

The CCRA is a worldwide agreement that has currently been signed by 28 nations. Ethiopia and Qatar were the last two countries to sign the agreement. The CCRA is very limited in terms of the audit depth of recognised certificates, but strengthens the Common Criteria as an international standard. The new version was released in version 3.1 revision 5 in April 2017. At the same time, version 4.0 of the Common Criteria will be worked on in Working Group 3 (WG 3) of Subcommittee 27 (SC 27) of the International Institute for Standardization (ISO) and the International Electrotechnical Commission (IEC) (ISO SC27 WG3), since the CCRA members could not complete the basic update without further support. The international industry is thus extensively involved.

SOG-IS INTENDED TO HARMONISE IN EUROPE

SOG-IS as a European agreement, on the other hand, is very much focused on harmonising the methodology of evaluation, thereby supporting national and European applications for certification. The agreement has been joined by 13 European countries so far, most recently Poland, Croatia and Luxembourg. Besides the technical domains in the area of "Smartcards and Similar Devices," the area "Hardware Devices with Security Boxes" has been strengthened in terms of harmonisation by the establisment of a subgroup for embedded devices (JEDS). Here, evaluation methodologies and qualification requirements for inspection bodies between the participants have been harmonised and the state of technology documented. In addition, close exchanges are held with representatives of the European Commission and the European Network and Information Security Agency (ENISA). This is intended to create transparency and support European projects, such as the establishment of a European IT security certification framework.

OBJECTIVES AND ACTIVITIES OF THE BSI

The BSI is committed to offering market-oriented certification options. This goal is achieved through close cooperation with the industry and the institutions responsible for the regulations.

By supporting equally low, medium and high test depths, the BSI enables customised certificates to be issued for different application scenarios and target audiences. For example, a manufacturer can also meet the procurement requirements of the USA. The BSI also takes this position for applications in Europe, in working groups on creating a European certification framework, for example. It thus contributes to the implementation of the European Directive on ensuring the high security of network and information systems (the NIS Directive).

Furthermore, the BSI proactively drives the harmonisation of crypto-evaluations using the Common Criteria – both in the CCRA for low test depths in order to offer an alternative to existing crypto-validations as well as in the SOG-IS for high test depths. In addition, the validity of the certificate of the certifying countries is being harmonised in CCRA and SOG-IS. ■

For more information see https://www.bsi.bund.de/Produktzertifizierung

SMART BORDERS

By Oliver Bausinger, Section Inspection Infrastructures and Architectures

EasyPASS system of the Federal Police at Munich Airport

The BSI Tests New European Entry/Exit System

According to the proposed regulation for the new entry and exit system (EES), any border crossing by a third-country citizen through one of the Schengen external borders is to be stored in a European register for up to five years. In addition to biographical data, a biometric photograph and fingerprints are also to be recorded. The BSI has been piloting the new processes of the EES together with the German Federal Police since 2015.

Right or left? This is the question travellers have to ask themselves when they come from a foreign country to a border control at a German airport or at another external border of the Schengen area. On the right, people can pass through who are entitled to freedom of movement from the existing 32 countries subject to the simplified entry and exit regulations. The left is intended for all third-country citizens who come from other countries. Some have to apply for an entry visa beforehand; others are allowed to enter the Schengen area without any pre-registration.

The Common Borders Code (named after the municipality of Schengen in Luxembourg, where the first agreement was signed in 1985) regulates the tasks and obligations of border control on entry into and departure from the Schengen area, and is directly applicable law for all participating states. It is of fundamental importance to comply with it, since within the Schengen countries there are no longer any checks on internal borders. In Germany, for example, the border controls are only carried out at air and maritime borders, but no longer at the country's borders.

EASYPASS – AUTOMATED BORDER CONTROL FOR PEOPLE ENTITLED TO FREEDOM OF MOVEMENT

Germany started to use automated security gates at all major airports in 2014. The EasyPASS system usually makes

Signing of the joint administrative agreements between the BSI, BPOL and BVA (2 June 2017 in Frankfurt)

Presidents of the BPOL and BVA and Department Director D together with those responsible for the project on behalf of the individual authorities in advance of the Smart Borders pilot installation at Frankfurt Airport

it possible to carry out the border crossing completely automatically. The digital photograph is scanned from the electronic chip of the passport and biometrically matched with a live-captured facial image. If the passport is cryptographically genuine and the identities match successfully, the traveller can pass the border without further manual testing by the border officer.

The BSI, in close coordination with the German Federal Police, regularly checks the systems for vulnerabilities, operates the necessary crypto-infrastructure within the framework of the National Public Key Directory and, with its guidelines, ensures that both document checking and biometric procedures always employ the latest technology.

NEW EUROPEAN ENTRY/EXIT SYSTEM FOR THIRD-COUNTRY CITIZENS

A new European entry/exit system (EES) is set to be introduced to bring handling of third-country citizens to a comparable level of security using a modern procedure. According to a proposal for an EU Commission regulation, which is expected to be adopted by the European Parliament in the fall of 2017, any border crossing of a third-country citizen through one of the Schengen external borders will be stored for up to five years in an EES. In doing so, not only the usual biographical data such as name, date of birth, etc. will be stored, but also a biometric photograph and four fingerprints. This is intended to enable much better identification of travellers. Multiple identities can then be identified by biometric matching. In addition, travellers who have exceeded their authorised period of stay can be easily identified.

EFFICIENCY THROUGH SELF-SERVICE

Since 2015, the BSI has been piloting new EES processes together with the German Federal Police. It soon became apparent that the entire border control process would have to change significantly with its introduction. The biometric reading of passengers directly at the counter, as well as the much more complex technical connections at airports over several levels up to the central EES, present considerable challenges for operating authorities in their effort to maintain both control depth and rapid passenger flow.

To counter these challenges, kiosk systems have been tested which would be placed ahead of border control areas. Travellers would carry out the document check, the detection or verification of biometric characteristics and the obligatory survey by the Border Police as self-service. They then proceed to the border control area where the officials have already received all relevant technical test results from the kiosk. In the final assessment, officials will usually only have to approve the border crossing. Within the scope of the pilot project, the BSI was able to prove that the time requirement remains roughly the same compared to the current procedure without an EES.

DIGITALISATION OF BORDER CONTROL

The introduction of biometric processes into border control processes highlights the importance of security for the systems in use. In the coming years, the BSI will help shape the technology development of border control, ensuring that new systems are operated reliably and safely. For this purpose, the BSI is entering into a project partnership with the German Federal Police and the German Federal Government to shape the technological challenges of secure border control. ■

For more information see https://www.easypass.de/

CYBER SECURITY

The BSI in Operation on Site

By Stefan Ritter and Timo Steffens, Section CERT-Bund

Examples of Mobile Incident Processing During Advanced Espionage Attacks

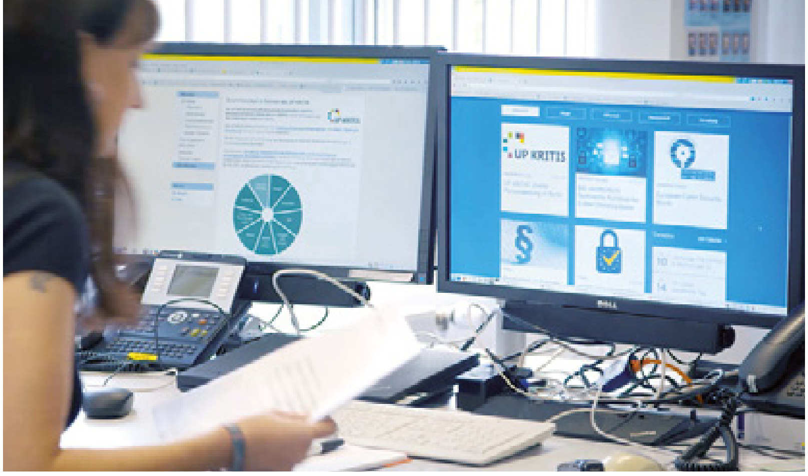
ADVANCED PERSISTENT THREATS (APTS)

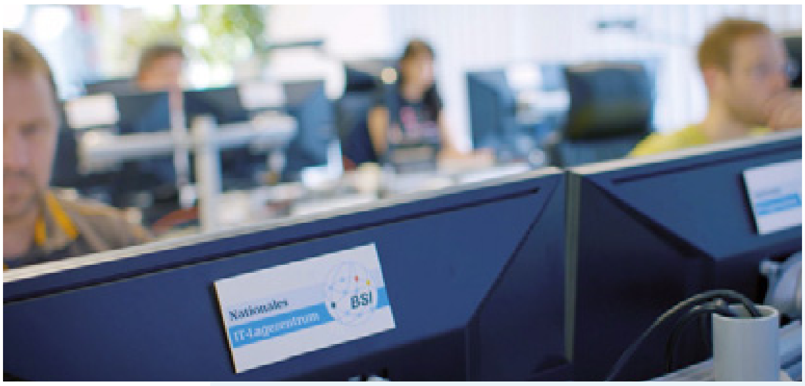
Advanced Persistent Threats (APT) are targeted cyber attacks on select institutions and facilities that allow an attacker to persistently access a network and subsequently expand it to other systems. The attacks are characterised by very high resource use and considerable technical abilities on the part of the attackers and are usually difficult to detect.

The call to the BSI Situation Centre comes in the afternoon. It is almost always this way since the affected person usually needs the morning to examine his own measures, recognise the huge challenge of the task at hand and finally get the approval of his superiors to turn to the BSI as an external third party.

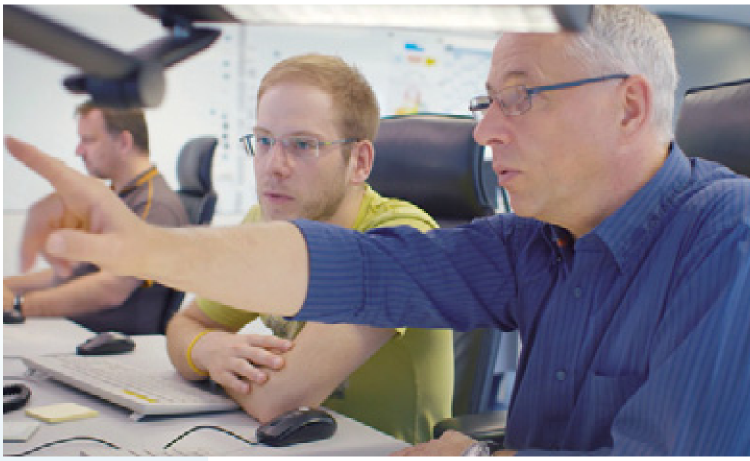
In this case, the IT security officer of a large SME is reporting an attack on the company's central IT, which the in-house experts are usually not able to cope with. It is – as in most of these cases – a serious attack against the company's crown jewels: production secrets, project planning, the communication of key personnel or attacks against confidentiality caused by so-called APTs (Advanced Persistent Threats).

Yet the company's responsible parties do not yet know this at the moment, nor do the consultants at the Situation Centre. It is clear from the first telephone call: there have been some anomalies with the internal IT for some time. A large unknown PST file blocked the e-mail outbox. And then it is noticed that the admin-employee who just carried out the change in the network has actually been on holiday for a week. The decision makers decide to seek external advice.





National IT Situation Centre of the BSI



The CERT-Bund employee calls the affected person in the early morning. He is trying to get an IT security officer or other IT-related management person responsible who can understand and deal with the problem. Personal conversation on the phone is important to ensure that the message arrives at the right place and is taken seriously and tracked.

The call was preceded by a report from the SIGINT Support for Cyber Defence program of the Federal Intelligence Service: a German company is suspected of being the victim of an APT attack. Like the BND, other news services also monitor servers and systems of attackers and analyse their attacks. If a company or an authority from a partner country stands out by communicating with such a system, this country – in this case via the BND and then the BSI – is informed in an appropriate way. In other cases, the message is sent by the CERT-Bund (Computer Emergency Response Team) its security-community and its contacts to the international CERT and security community. In the first telephone call, the BSI clarifies the plausibility and background of the message with the company concerned and tries to get initial supplementary information on the incident.

INCIDENT REPORTS

Incident reports come to the BSI Situation Centre in various ways, primarily various reporting procedures for the Federal Government according to Section 4 of the BSI Act, the reportable critical infrastructures according to Section 8b and the public reporting office of the Allianz für Cybersicherheit. In addition to such written, formatted and unformatted messages, calls are often made.

DEPLOYMENT DECISION

After comparing the existing information and the exchange of contacts, a further timely telephone conference is agreed between the employees of the Situation Centre or the CERT-Bund and the parties responsible in the affected institution. Experts from various disciplines of the BSI take part. Further details and backgrounds, symptoms and possible effects are discussed. After a case-by-case examination, the BSI then decides whether the solution cannot be supported solely by further advice and aids (such as good practice documents, reference to consulting firms, etc.) or forensic support, or whether an on-site visit is necessary, a so-called MIRT (Mobile Incident Response Team) assignment. Depending on the urgency of the assignment, the basic conditions and the personnel availability, a team will be sent as soon as possible.

OPERATION ON SITE

In this case, the BSI experts find good conditions: the company concerned has already created the framework conditions to receive support from the BSI. These include the availability of the right contacts and the necessary data such as network surveys, log data, etc. After a preliminary meeting on site in which the problem and the technical situation are discussed again in detail, a joint deployment plan for the next steps is discussed.

The MIRT experts try first to isolate the problem and to isolate the cause of the damage. Tools are deployed to search for attacker signatures (so-called Indicators of Compromise, IoCs). The BSI provides its own confidential data from the protection of government networks, with which the signatures are compared. They look for further damage and impacts of the attack and isolate them as far as possible. How far and deep has the attacker worked into the network? Have central components already fallen? Has the attack possibly even found the “golden ticket” of the “master admin,” gaining full control over the entire network? Is it still active? Can anyone observe what it is doing and where exactly it is without losing important data? How is it connecting to the network? How is it exfiltrating its “prey”? Where could it set up traps and loops, e.g. over VPNs? Only if you know how and from where the attacker is acting can you safely lock it out.

This results in the possibility of implementing a largely secure transition operation after completion of the analysis phase in order to ensure basic workability in the institution. Parallel to this, in cooperation with an external service provider, planning is made on how the network can be designed as quickly as possible to ensure that further attacks are not possible in the short term. The MIRT experts are constantly discussing this with local experts as well as with their other colleagues at the BSI.

Technical and forensic analytics take time. In the following days, analysis phases in the BSI and phases of the work on site often alternate. New findings have to be introduced into the investigation and the search sequences has to be continuously restarted.

COOPERATION BETWEEN THE BSI, THE SECURITY AUTHORITIES AND OTHER CERTS

The BSI does not stand alone in the support of those concerned. It reports with pseudonyms – that is, WITHOUT mentioning the name of the person concerned – and with a high level of abstraction to the security authorities in the Cyber Response Centre. Other authorities are informed about the basics of the incident and can provide their own information.

Contact by the BSI’s partner organisations with the party concerned is made exclusively in consultation. This method of cooperation is often worthwhile for the institutions concerned. For example, an investigation can be initiated by the Federal Criminal Police Office or by the Central Cybercrime Contact (ZAC) of the State Criminal Police Offices in order to gain better insights into the protection of the networks and data, as well as to enable the identification

Left: Mobile Incident Response Teams (MIRT) on the way to the scene of operations

Below: MIRT operations on site to limit damages

of perpetrators and their arrest and prosecution in the long term. The involvement of the Federal Office for the Protection of the Constitution can also help to get further information on protection and to identify the perpetrators.

The BSI also shares technical parameters and IoCs for attackers and perpetrators with national and international CERT partners – as well as anonymously for affected parties, passing on as little framework information as possible. The assistance provided by the BSI for the detection and analysis of an incident and partly from the other CERT partners is enriched with data from current incidents and can be used to assist others just as they helped the party concerned. There is also the possibility that the BSI may, in consultation with the party concerned, be supported by consulting firms or other external experts if the need arises.

D-DAY / CLEAN-UP

At a certain point in time called "D-Day," after networks have been completely compromised for several weeks, they are completely shut down and then restarted again for cleaning. All passwords are reset and the system is "clean" when it re-enters operation. This is followed by an intensive observation as to whether the attacker has succeeded in "hibernating" through the clean-up with backdoors and is trying to spread out again in the network.

FINAL MEASURES

Immediately after D-Day, the BSI supports the affected party in setting up an internal project that makes the network and its processes resilient against attacks in the long term. This is to prevent successful infections of individual clients from causing the whole network to "fail" in the future. In the short period of provisional additional defences and reestablishment, it is often not possible to implement all necessary changes (e.g. two-factor authentication for admins, segmentation, APT attack detection, etc.).

In a follow-up meeting with all participants and the subsequent follow-up work in the BSI, the findings and experiences are collected and arranged in order to be prepared for the next assignment and to be helpful for other affected parties. For this, for example, the internal checklists are revised and new tools are procured. If possible, findings are shared with other security teams without mentioning the name of the person concerned, because, when the telephone rings the next time in the late afternoon, the employees of the Situation Centre have to be prepared as well as possible. ■

JULY 2015
IT SECURITY ACT ENTERS INTO FORCE
§
MAY 2016
FIRST PART OF THE BSI KRITIS REGULATION ENTERS INTO FORCE
§

LEGAL BASIS UPDATED

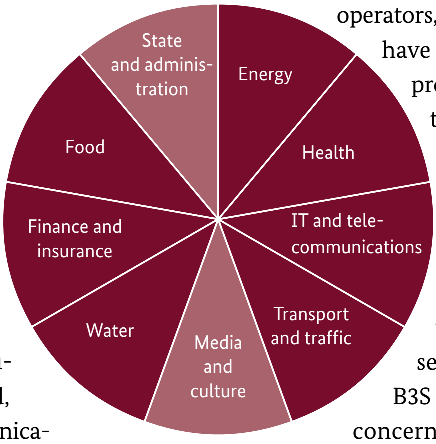
By Nora Apel, Section Director Critical Infrastructures – Principles

Implementation of the NIS Directive Reaches Further Milestones

End of June 2017 the NIS Directive Implementing Act entered into force. The European Directive adopted in July 2016 realises “measures for ensuring a high common level of security of network and information systems,” in Germany. In June 2017, the second part of the BSI KRITIS Directive entered into force. This concludes a legislative process that began with the IT Security Act in 2015.

ALL KRITIS SECTORS REGULATED

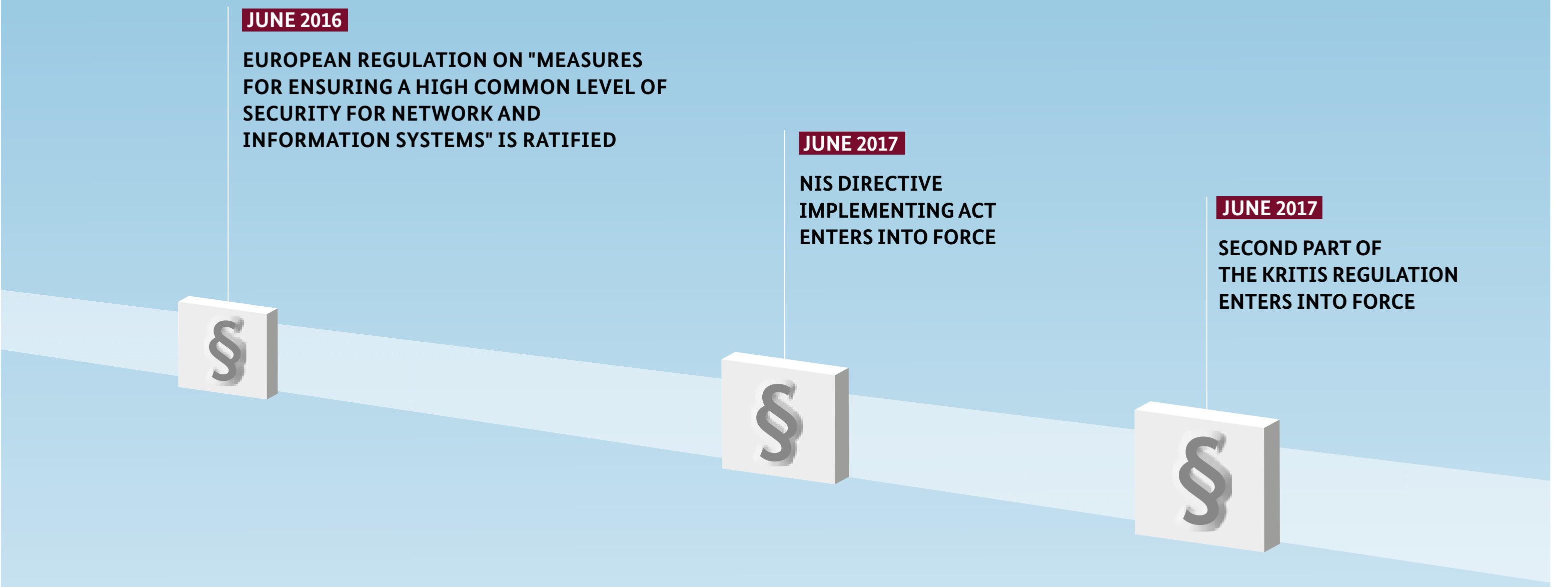
The act on increasing the security of information technology systems (IT Security Act, IT-SiG) entered into force on 25 July 2015. It amended, among other things, the BSI law that certain future Operators of critical infrastructures are committed to a minimum level IT security and to prove it against the BSI, as well as to report significant IT security incidents to the BSI that either have or could have an impact on critical infrastructures.



Who exactly is covered by the law is regulated by the corresponding legal directive (BSI KRITIS Directive, BSI KritisV) issued in accordance with § 10 BSIG. Quantitative and qualitative criteria are used to determine who is affected by the new regulations. The legal directive was adopted in two parts, or “baskets.” The first basket entered into force on 3 May 2016, regulating the sectors of energy, water, food, information technology and telecommunications. The second basket entered into force in the form of an amendment of the existing BSI KritisV on 30 June 2017. It regulates the remaining KRITIS sectors of health, transport and traffic, as well as finance and insurance, and makes some concretisations and changes to existing regulations. The media sector, which is also one of the critical infrastructures, is not affected by the law, as the Federal Government has no legislative authority here (see illustration of sectors).

COOPERATIVE IMPLEMENTATION

The implementation of the act is being carried out cooperatively as part of the UP KRITIS platform in which KRITIS operators, associations and competent authorities have been cooperating voluntarily on the protection of critical infrastructures for ten years already. In various bodies of UP KRITIS, a decision is made on how the reporting obligation is to be shaped, and so-called “industry-specific security standards” (B3S) are developed with which the “state of the art” is concretised regarding IT security in the various industries. The B3S is an opportunity for the operators concerned to formulate the state of the art in detail based on their own expertise. On request, the BSI examines the suitability of this B3S in consultation with the Federal Office of Civil Protection and Disaster Assistance (BBK) and the responsible supervisory authorities.



JUNE 2016

EUROPEAN REGULATION ON "MEASURES FOR ENSURING A HIGH COMMON LEVEL OF SECURITY FOR NETWORK AND INFORMATION SYSTEMS" IS RATIFIED

JUNE 2017

NIS DIRECTIVE IMPLEMENTING ACT ENTERS INTO FORCE

JUNE 2017

SECOND PART OF THE KRITIS REGULATION ENTERS INTO FORCE

Operators set to be audited in accordance with such an approved B3S will have legal certainty regarding the “state of the art” required and reviewed in an audit. However, there is no statutory duty to develop or apply a B3S.

The opportunity to develop a B3S and to therefore be able to co-determine what is considered the “state of the art” in the individual KRITIS sectors with regard to IT security is actively used by the industries in the UP KRITIS. The B3S “Water/Wastewater” for the sectors “Public water supply” and “Public wastewater disposal” was the first to be classified as suitable by the BSI. Further B3Ss are currently being developed and are due to be finalised in 2017.

However, the IT Security Act not only provides obligations for KRITIS operators, but rights as well. The BSI is obliged to provide KRITIS operators with information on security gaps, malicious programs, successful or attempted attacks and the respective observed approach as well as a continuous situation status.

NIS DIRECTIVE IMPLEMENTING ACT ADOPTED

“Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for ensuring a high common level of security of network and information systems across the Union” (NIS Directive implementing act) has again expanded the tasks and competencies of the BSI. In the future, the BSI can, for example, check compliance with the requirements of Section 8a (1) BSIG at local operators.

The scope of the operators affected by the act also extends through the NIS RL implementing act. From now on, the reporting obligation and the implementation of the state of the art in IT security (section 8c) will also apply to providers of digital services such as search engines, cloud services and online marketplaces. In addition, the Telecommunications Act (TKG) has introduced regulations which allow operators of telecommunications networks to respond to attacks.

At the same time, KRITIS operators are also given new support by this directive. For example, the BSI may support operators locally, for example, in the case of prominent IT security incidents, in order to restore the security or functionality of the affected information technology system.

Both the 2015 IT Security Act and the NIS RL Implementing Act of April 2017 provide a new foundation for the collaboration between the BSI and critical infrastructure operators. The acts continue the cooperative approach of the protection of critical infrastructures that has been pursued for many years, and has resulted in a “win-win” situation for operators and the state. ■

For more information see https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS-Richtlinie.html

IT-GRUNDSCHUTZ REDESIGNED

By Katrin Alberts, Section IT-Grundschutz

Information Security for Business and the Administration

Thousands of hours of professional processing of individual publications, dozens of workshops with IT users from administration and companies as well as numerous internal discussions and votes at the BSI: the modernisation of IT-Grundschutz is a large-scale project. At it-sa 2017, this work will be summarised in a presentation of new BSI standards and the new IT-Grundschutz compendium. This content is now available in a compact and clear form for various target audiences. Users can use it to build a management system for information security in their institutions.

IT-GRUNDSCHUTZ – THE ORIGINAL REGARDING INFORMATION SECURITY

New BSI standards and building blocks, a new IT-Grundschutz compendium: after an intensive phase of technical revision, the proven IT-Grundschutz method, now updated and modernised, is available for IT-Grundschutz users and new prospective customers. Whether an agency's Information Security Officer, a large company's Chief Information Security Officer (CISO) or the Managing Director of an SME: they are all able to provide appropriate security information in this new IT protection offer to meet the requirements of their institution. The security information in the various publications covers: What is the current status of an institution's information security? What areas need action? What measures can be taken to increase the security level in the short term? What measures require a longer planning process and more resources?

IT-Grundschutz provides a modular and flexible method for beginners and advanced users to handle information security. Users can select different offers that they can work with in their institution based on their prior knowledge. In the new IT-Grundschutz compendium, a large part of the necessary new building blocks that can be used to increase an institution's information security has been published. This is one of the most important objectives of the entire modernisation process. For IT users, there are moderate deadlines for migrating "old" IT protection to the modernised content. This also applies to all questions relating to certification.

NEW CONTENT – MANY TARGET AUDIENCES

In addition to the IT-Grundschutz compendium, new BSI standards on individual focus areas have also been published. The BSI standard 200-1 defines general requirements for an information security management system (ISMS). With the BSI standard 200-2 on the IT-Grundschutz methodology, the basis can be laid to build a solid ISMS. The BSI standard 200-3 for risk management contains all risk-related work steps in the implementation of IT-Grundschutz. New in the offer portfolio is a "guide to basic protection." The new publication is based on the BSI standard 200-2 and describes how smaller companies and authorities can implement basic protection in a targeted manner.

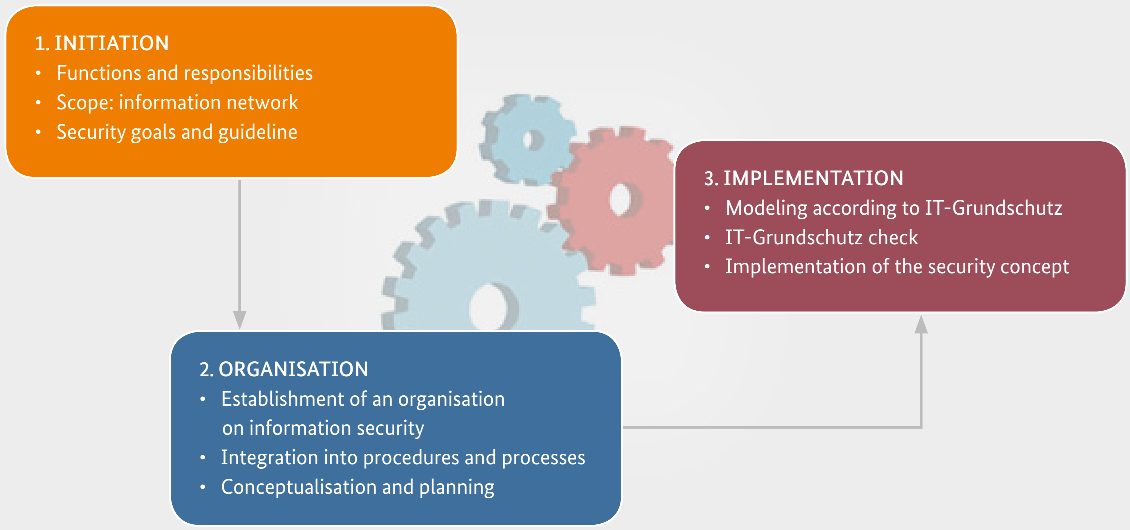
The modernisation of IT-Grundschutz content has taken place in close cooperation with the IT-Grundschutz community. Current content can be checked by users during actual practice and their feedback can be processed even more effectively. This exchange has proven to be very valuable, both for individual publications as well as for strengthening the community concept of IT-Grundschutz itself.

INFORMATION SECURITY AS A PROCESS

If IT-Grundschutz has also been fundamentally revised by means of modernisation and the content has been updated to the state of the art, the process reliability and the development potential in information security mean that IT-Grundschutz has to be continually updated. Existing publications must be reviewed and new building blocks must be developed. Revision of the existing BSI standard 100-4 for emergency management is planned in the future. A completely new standard on measurability is also under discussion. IT-Grundschutz will continue to face dynamic challenges in the future, and the BSI, together with IT-Grundschutz users, will stay committed to it. ■

GUIDE TO BASIC PROTECTION

The three phases of the security process



1. INITIATION
- Functions and responsibilities
- Scope: information network
- Security goals and guideline

2. ORGANISATION
- Establishment of an organisation on information security
- Integration into procedures and processes
- Conceptualisation and planning

3. IMPLEMENTATION
- Modeling according to IT-Grundschutz
- IT-Grundschutz check
- Implementation of the security concept

For more information see https://www.bsi.bund.de/grundschutz

New Minimum Standards

By Dominique Hader and Philipp Deuster, Section Minimum Standards for the Federal Administration

Continue to Strengthen Cyber Security

Mindeststandard des BSI für sichere Web-Browser

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 20.03.2017

Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden

1 Satz 1 BSIG

Mindeststandard des BSI für Mobile Device Management

8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 11.05.2017

Mindeststandard des BSI Nutzung externer Cloud

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 24.

Mindeststandard des BSI für Schnittstellenkontrol

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 16.11

Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 3.0

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 26.05.2017

The BSI as the national cyber security authority is developing minimum standards for the security of the information technology of the Federal Administration in Germany. The basis for this is § 8 (1) of the BSI Act. The definition is based on the BSI's professional expertise in the conviction that at least this minimum level is achieved in the Federal Administration. Current developments in information technology require the updating of the standards over time or the development of completely new standards.

In 2014, the BSI published the minimum standard for the use of the SSL/TLS protocol as the first document of its kind. Since then, much has been done. Among other things, the task of establishing minimum standards was further strengthened by the 2015 IT Security Act. The central objective of these legally enshrined requirements is to define a concrete minimum level of information security for Federal Government bodies. Of course, other users from the state, business and society can also use the guidelines as a benchmark for the security of their own systems. At present, there are minimum standards for the following six topics:

- The use of the SSL/TLS protocol
- Interface controls
- Secure web browsers
- The use of external cloud services
- Mobile device management
- Application of the HV benchmark compact 3.0

STANDARDISED APPROACH

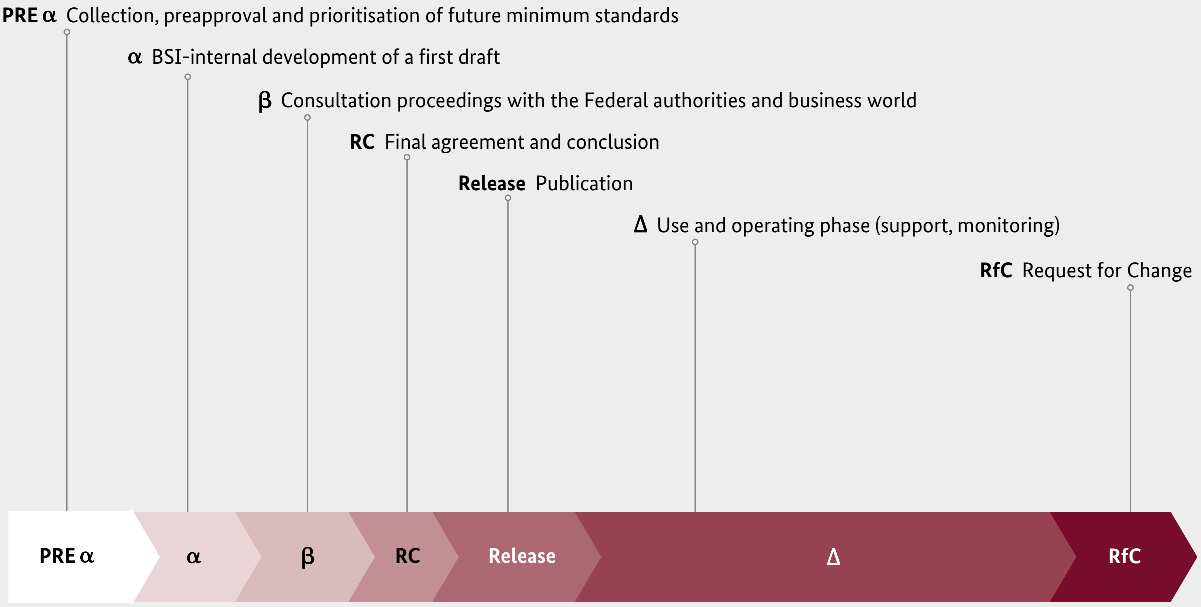
IT systems are usually complex and characterised in their individual application areas by a wide variety of framework conditions and requirements. This not only creates challenges for users to secure their IT. The BSI also must face the task of developing appropriate guidelines for this comprehensive subject. The development path of the minimum standards established so far already shows the professional diversity of the subject areas. Different specialist sections and expert circles in the BSI are therefore assigned to each minimum standard. For this reason, the creation process requires a high degree of cooperation between all the experts involved, including the user's side in the Federal Government.

In order to ensure effectiveness and efficiency in the preparation and maintenance of minimum standards, this process is described in detail in a standardised approach (see figure on page 24). Within the framework of quality assurance, each minimum standard runs through several test cycles:

- Collection of ideas (PRE-α): Not only the BSI develops thematic proposals, but also the users can contribute their wishes and ideas. This provides the opportunity to involve the target audience with its professional expertise already from the beginning.
- BSI internal coordination (α): If a topic for a new minimum standard has been selected from the collection of ideas, the first draft is initially approved by the BSI. In this case, not only the relevant expert section is involved, but all departments have the opportunity to participate in developing the draft.
- Consultation process (β): Similar to the beta phase in software development, users are invited to "test" the β version of the minimum standard. To this end, the draft is submitted to them for comment and they can again introduce their own experiences.
- Final reconciliation (release candidate): After the external comments on quality assurance have been included, the minimum standard is approved for release.
- Utilisation and operating phase (Δ): In this phase, users are supported (support) and the effectiveness and efficiency of the minimum standard is monitored (monitoring). Any changes (request for change) are recorded and, if necessary, incorporated.

Such an extensive, quality-oriented process, of course, takes time. Depending on the scope of the topic, the availability

LIFE CYCLE OF MINIMUM STANDARDS



PRE α Collection, preapproval and prioritisation of future minimum standards

α BSI-internal development of a first draft

β Consultation proceedings with the Federal authorities and business world

RC Final agreement and conclusion

Release Publication

Δ Use and operating phase (support, monitoring)

RfC Request for Change

of experts and various other factors, it will take about half a year from the beginning of development to the completion of a new minimum standard.

As important as the minimum standards are, however: They are always only a hedge downwards. In practice, requirements for information security become regularly higher than those described in the minimum standards. Based on the minimum standards, the users have to consider these individual requirements in the planning, establishment and operation of the IT systems in order to meet the respective requirements for information security. The IT-Grundschutz standards of the BSI describe this approach.

PART OF THE CYBER SECURITY STRATEGY

Minimum standards are an essential part of the cyber security strategy for Germany. In the strategic fields of action "Safe and self-determined action in a digitalised environment", "joint order of the state and economy" as well as "Efficient and sustainable general government cyber security architecture," they enable a minimum level of security for the information technology of the Federal Government to be achieved by providing clearly defined standards. In addition, they are a connecting element in two respects: on the one hand, they are not produced as isolated publications, but it is considered very important for them to have a relation to other publications of the BSI (e.g. to the requirements catalogue C5). On the other hand, a targeted comparison is promoted through the participation of the various bodies in the creation process.

The BSI is currently working on minimum standards for the use of cloud services, for the logging and detection of cyber attacks, for user obligations within the framework of protection of the inter-departmental communication infrastructure, and for the application of the modernised IT-Grundschutz. ■

For more information see https://www.bsi.bund.de/mindeststandards

TRUSTING COOPERATION

By Joachim Gutmann, Glücksburg Consulting AG

First IT Security Platform for Industrial SMEs

Small and medium-sized enterprises (SMEs) often lack the resources to deal with cyber attacks with specialised teams called Computer Emergency Response Teams (CERT). They must increasingly open themselves up to inter-company cooperation. Trust is absolutely crucial for this. The Association for Electrical, Electronical & Information Technologies (VDE) has now found a solution: a CERT platform.

The digital transformation towards Industrie 4.0 opens up great opportunities and value-adding potentials – especially for growth-driving SMEs. At the same time, however, the risk of cyber-attacks is increasing with the progressive connectivity of production facilities with modern information and communication systems (ICT). Threats range from system and production failures through malfunctions with accident sequences to industrial espionage and sabotage. The possible consequences are therefore serious.

For this reason, it is all the more important to strengthen IT security as a critical success factor for Industrie 4.0 and digitalisation: firstly, by improved prevention in system development, secondly, by the fastest possible detection of new vulnerabilities, and thirdly, through a systematic and coordinated response to attacks.

And this is where CERT@VDE comes in: the first platform for coordinating IT security problems especially for SMEs in the field of industrial automation. “Our platform provides manufacturers, integrators, plant builders and operators in the field of industrial automation the opportunity to exchange information intensively and confidently,” says Andreas Harner, Head of VDE-CERT. The platform developed by the VDE committees and developed by industry members of the association was presented for the first time at the Hannover Messe Industrie.

AWARENESS IS THE FIRST STEP

The results of the 2017 VDE Tec Report, a survey among the 1,300 VDE member companies and universities, show how important this topic is for SMEs. According to the survey, 88 % of interviewees are convinced that IT security is a key pillar of successful digitisation. And almost all (93 %) consider critical infrastructures – in the energy sector, for example – in need of particular protection. More than half of respondents (53 %) had already been affected by cyber-attacks, while large companies (71 %) and major universities (68 %) were attacked clearly above average online. Research and development (78 percent), IT/software (70 %), production (57 %) and planning/project planning/engineering (40 %) are particularly at risk.

IT SECURITY IN THE TECHNOLOGY POLICY AGENDA

Awareness certainly exists, but in the implementation of the findings, the weak point with many SMEs is still in industrial automation. While large national and international companies and institutions usually have their own CERT to coordinate the handling of vulnerabilities in their own systems and to provide IT security information in a structured manner, SMEs generally lack these resources. Many SMEs do not even have a developed IT department, let alone the capacity for specialised emergency teams. And even where these have already been established, there is a lack of structures for trusting cooperation with other manufacturers. “In order to foster this necessary trust,” VDE security expert Harner explains, “we have agreed to fixed guidelines for the platform that are valid for all participants.” A confidentiality agreement serves as the basis for collaboration on the IT security platform. The guidelines make this agreement concrete and determine the cooperation with CERT@VDE:

- The confidentiality of customer data is to be given top priority.
- Cooperation is voluntary and can be terminated at any time.
- Business models of individuals may not suffer from CERT@VDE activities.
- By means of reciprocal contributions and information, the workflows of all members are to be optimised.
- Information and the interests of other members are to be protected.

At regular working meetings with platform participants, these guidelines are fulfilled in reality and enriched by personal trust.

BUILDING A KNOWLEDGE PLATFORM

Unlike already existing CERTs in Germany (for example, the CERT Federation of the BSI, which acts as a central point of contact for all problems in computer systems), the VDE security initiative specialises in the field of industrial automation. “But, of course, we are looking for collaboration with other CERTs and the CERT-Bund,” says Harner. “Learning from one another is not only the highest maxim for the participants in the CERT@VDE, but also in general.”

The security platform enables a cross-vendor exchange on a neutral, trustworthy and secure platform – while maintaining anonymity. Formerly isolated information is centrally bundled, structured and distributed in the

Profile in brief:

Joachim Gutmann is a freelance journalist and author. He has spent his professional career in Berlin, Bonn, Düsseldorf, Gummersbach and Hamburg and the last 17 years working as a communications expert for Glücksburg Consulting AG.

THE SECURITY PLATFORM ENABLES A CROSS-VENDOR EXCHANGE ON A NEUTRAL, TRUSTWORTHY AND SECURE PLATFORM.

CERT@VDE, so that different industrial participants always have the same, up-to-date knowledge regarding security standards and hazards. Access to the platform, which can also be used as a knowledge database, is provided by customer-specific access. In the future, a cockpit user interface will allow for the collection and arrangement of security topics of relevance to users. Companies that are affected by an attack can also ask IT experts to assess the situation on short notice and benefit from their help.

"We create efficient and effective cooperation structures for IT security and production managers that enable us to work together to meet the high security risk that has become the central challenge to Industrie 4.0," says Andreas Harner.

CYBER SECURITY FOR A SUCCESSFUL DIGITALISATION

The platform serves as not only the central know-how centre for dealing with vulnerabilities, however, but also facilitates their timely processing. For the participants, target audience-oriented vulnerability information from various sources is also prepared and made available. In addition, support for closing security gaps is coordinated via the platform.

Coordination and communication are, in every case, the two guiding principles under which the platform operators approach their tasks. The platform is used to organise the cross-company exchange of security problems in protected interaction rooms and to encourage the exchange of suitable approaches. For participants in the automation industry, workshops are offered and best practices are worked out together with partners.

"If SMEs want to compete with the big players in the industry," says Harner, "they have to tear down the walls of fear in a protected atmosphere and start learning from each other." Only from learning together will faster assessments of incidents take root and effective mitigation be addressed. ■

ABOUT THE VDE

With 36,000 members (including 1,300 companies), the VDE is one of the largest technical and scientific associations in Europe. In addition to its CERT platform, the VDE runs the VDE/DKE contact point for information security (KSI) and carries out related research for the BMBF projects "Connected IT Security Critical Infrastructures (VeSiKi)" and "Reliable Wireless Communication in Industry (BZKI)." With the IEC 62443 series of standards "Industrial Communication Networks – IT Security for Networks and Systems" and the standard roadmaps "IT Security" and "Industrie 4.0," the VDE/DKE, which also organises the Standardisation Council for Industrie 4.0, is driving the standardisation of IT security and Industrie 4.0. In the area of testing and certification, the VDE test institute offers the VDE certificate that confirms that information security has been tested.

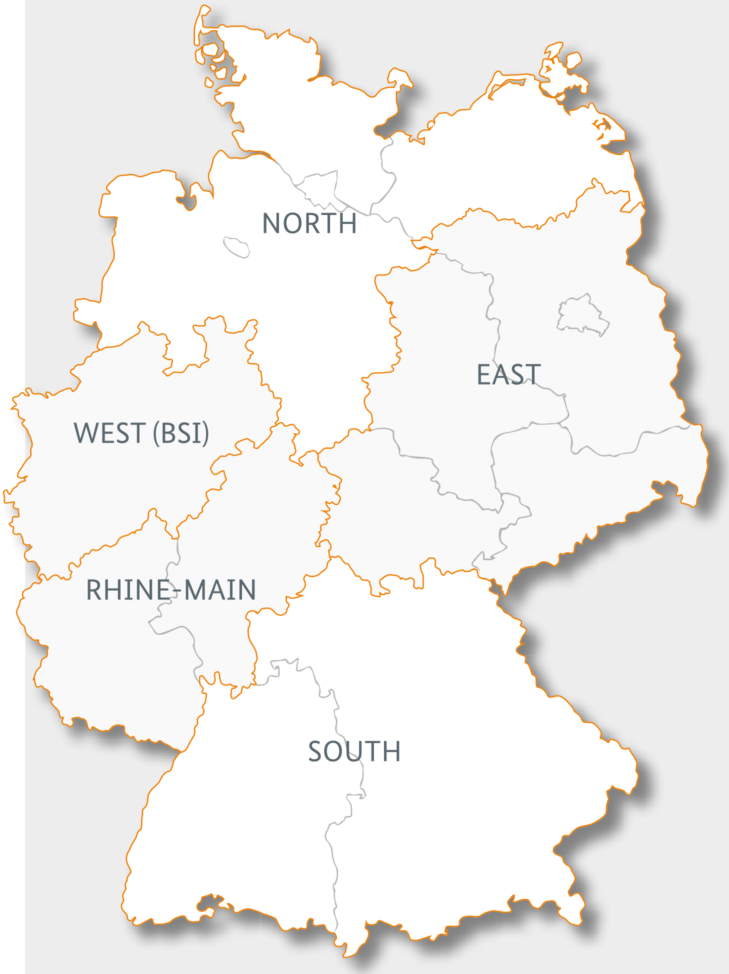
THE BSI

BSI on Site

By Fabienne Middeke, Section National Liaison Office

BSI to Set Up Regional Liaison Offices

As a national competence centre for cyber security, the BSI pools professional and operational expertise. The number of its customers and partners is growing. But how can this expertise be made available in a uniform structure for the target audiences of state, the business world and society? Since the beginning of 2017, a new area in the BSI has been on the case – the National Liaison Office.



Coverage and support to the federal states through the envisaged liaison offices of BSI

The BSI is growing, and not just in terms of personnel; as a national cyber security authority, the office is being assigned more and more responsibilities. In addition to maintaining classical BSI contacts with federal authorities, companies, associations and think tanks, the National Liaison Office is also responsible for extending the BSI's competence to the regions through liaison offices. In the business world, it is also responsible for "hidden champions" and in the area of government, for the federal states and international organisations based in Germany.

BSI MESSENGERS ON SITE

In order to be able to fulfil its various tasks on the ground, the BSI has begun to establish regional branch offices. The offices will initially cover cross-country regions or metropolitan areas, in perspective, the BSI is setting up a total of five liaison offices – four of them in Germany and one in Belgium. Preparation work began in 2017 with locations in the Rhine-Main region and Berlin. The pilot operation has already started successfully, with the offerings from the BSI and its regional offices in great demand from various target audiences.

An international liaison office will be opened in Brussels and an office in southern Germany in 2018. In early 2019, a liaison office in northern Germany is set to follow. With the expansion of its liaison office, the BSI is extending its cooperation model with the state, the business world and society into yet another dimension.

As a rule, liaison officers reside at partner organisations and institutions in their respective regions. Currently, the Federal Criminal Police Office (BKA) in Wiesbaden and the Federal Statistical Office (Destatis) are significantly contributing to the success of the new BSI liaison office through their logistical support.

BSI employees are available in person as contacts several days a week and and are available to answer questions about BSI and cyber security. They can also be a first point of contact for technical questions. And in case of specific technical questions, they have direct connections to relevant contacts in the BSI, facilitating access to the BSI as a national competence centre for cyber security. They also advise target audiences on BSI products and services.

START IN THE RHINE-MAIN REGION

As a metropolitan area, the Rhine-Main region is an ideal starting point for expanding connections with a number of authorities and companies, some international authorities are based there. The BKA is an outstanding partner and cooperation is an important focus here. The BSI cooperates with the BKA in the National Cyber Defence Centre, for instance, and as a partner in the German Competence Centre against Cyber Crime e.V. (G4C).

The federal states of Hesse, Rhineland-Palatinate and Saarland are supported from Wiesbaden. But companies as well can address cyber security questions to the liaison office. In the Rhine-Main region, Darmstadt Technical University is an important science centre with a research focus on IT security. Here too, the liaison office supports networking with the BSI. The BSI provides “host nation support” for international organisations based in Germany. This also applies to international authorities in the Frankfurt area.

Roland Hartmann, Head of Section National Liaison Office (3rd from left) and Fabian Weber, Liaison Officer in Berlin (2nd from left) open the Liaison Office in Berlin while also welcoming a delegation from the Cyber Security Agency (CSA) from Singapore

FOCUS ON THE FEDERAL STATES

As the national cyber security agency, the BSI will continue to strengthen the expertise it makes available to the federal states. Germany’s 2016 cyber security strategy lays the groundwork for closer cooperation between the federal states based on stronger partnerships between states and government, tasking the BSI with assisting state authorities in coping with cyber incidents. This has been legally assured with the BSI Act that was recently amended as part of implementing the European NIS Directive.

The federal states are mainly supported at three levels: operationally in the German government CERT alliance; through information security consulting services; and regionally with the support services of the liaison office. The BSI provides the federal states with expertise, best practices and products, but that does not replace investing in necessary cyber security competences and resources at the state level.

CONTACT

It is already clear in the successfull pilot phase that the BSI’s new regional focus is the right path to meet the current challenges in cyberspace, decentralising BSI expertise to make it available as a national cyber security agency. Individual aspects will be in focus in the other locations of its select regions as well. Get in touch with the liaison offices in the Rhine-Main area and Berlin by email: **BSIregional@bsi.bund.de**. ■

Cyber Security in Digitalisation

By Arne Schönbohm, President of the BSI

BSI – Shaping Cyber Security Impartially

Digitalisation has become an important basis for technological progress as well as for economic and social prosperity. This includes administrative procedures, such as electronically applying for education grants (BAföG), fully automated processes in industrial production or online bank transfers over mobile phones. Nevertheless, the challenges are also growing with ever-increasing connectivity: the complexity of IT continues to grow, providing cyber attackers with a wide range of opportunities to spy out information, sabotage business and administrative processes or criminally enrich themselves using various methods at the expense of others.

It is the duty of the state to create and maintain security even in cyberspace for its own democratic administrative institutions, the economy and its citizens. With this goal in mind, the Federal Office for Information Security was founded by the Federal Government more than 25 years ago. Since then, it has developed analogous to the further development of technologies into a central competence centre. The enormous increase in staff this year by 30 percent to 850 employees across all departments is evidence that the BSI is recognised and strengthened in its role as the national cyber security authority.

This increase in staff will enable the BSI to better position itself in many areas – also supported by an organisational reorganisation. For example, since the beginning of the year, a dedicated department has devoted itself to the subject of “cyber security in digitalisation.” IT security specialists are involved in topics such as the energy revolution, the Internet of Things (IoT) and Industrie 4.0 at the national and international levels.

With the reorganisation and the high number of new staff, the BSI is taking account of the changing requirements a national cyber security authority must meet. We understand that information security is the prerequisite for digitalisation and are shaping information security. This is only possible by taking a broad cooperative approach, which has been practiced for many years at the BSI. It does not only involve close cooperation with external partners from business, science and administration, but, in particular, the interdisciplinary connectivity of the employees from various disciplines. From cryptography as basic research up to concrete practical offers such as IT-Grundschutz or the CERT-Bund, all the necessary competences for dealing with highly complex questions are combined at the BSI. This is the unique feature of the BSI.

The spectrum goes a lot further. A daily situation report, for example, is created and evaluated together at a daily briefing by the different departments in the National Situation Centre. If abnormalities are detected during the evaluation or in daily operations, established internal and external reaction pathways take effect. Messages for the affected target groups are created and tailor-made cyber defences are initiated and implemented in direct contact or by Mobile Operational Response Teams (MIRT).

“We understand that information security is the prerequisite for digitalisation.”

This was also the case in the middle of May, when the first infections with the ransomware “Wannacry” were observed. After an internal evaluation and the exchange with national and international partners, the BSI contacted the affected parties. From the information received from them and technical expertise, we were able to write and send warnings to our customers in government, the business world and society. From the findings that are drawn in the follow-up of an incident, short-term preventive tasks, such as consulting services, products or formulations of standards, are carried out in order to comply with the state of the art. In the current case, the BSI provided antivirus signatures for AV scanners and a dossier for protection against ransomware and adapted its awareness offers for the target audiences from government, business and society to the current situation.

In addition, these incidents are always an occasion to draw attention to the BSI’s strategic demands, as in this case, on minimum standards and the obligations of companies for their IT products. The establishment of a first quality seal planned for the coming year, as required in the Cyber Security Strategy, will be set as a milestone.

This fast, proven and effective approach would not be possible without the cooperation of all the colleagues involved in the BSI together with its national and international partners.

According to our findings, a large number of such incidents can be expected in the future, which will not honour vital institutions or national borders – the increasing digitalisation of all areas of life leaves no other conclusion. This makes it all the more important to have close international cooperation, independent expert knowledge in the area of digitalisation, as well as reasonable risk management that includes cyber security. Only a holistic approach to information security makes digitalisation successful in all areas of life.

Due to its synergies and processes, these competences and partnerships are in good hands at the BSI. Success models clearly show this, with BSI IT-Grundschutz as the national standard for information security, for instance. But the further development of the BSI’s crisis responsiveness is also part of this with a new line-up for the Cyber Defence Centre. Through this central position, we are pursuing the goal of becoming a “thought leader” on sending essential impulses for cyber security in the design of digitalisation.

We assume that the resources for the BSI will also increase parallel to the growth of the importance of the topic. We have been able to prove that resources are in good hands at the BSI, with the filling of more than half of the allocated positions already in the first half of the year.

The BSI – Networked Competence in Cyber Security

The Example of Incident Processing as an Integrated Value Chain

Prevention

Strategic situation

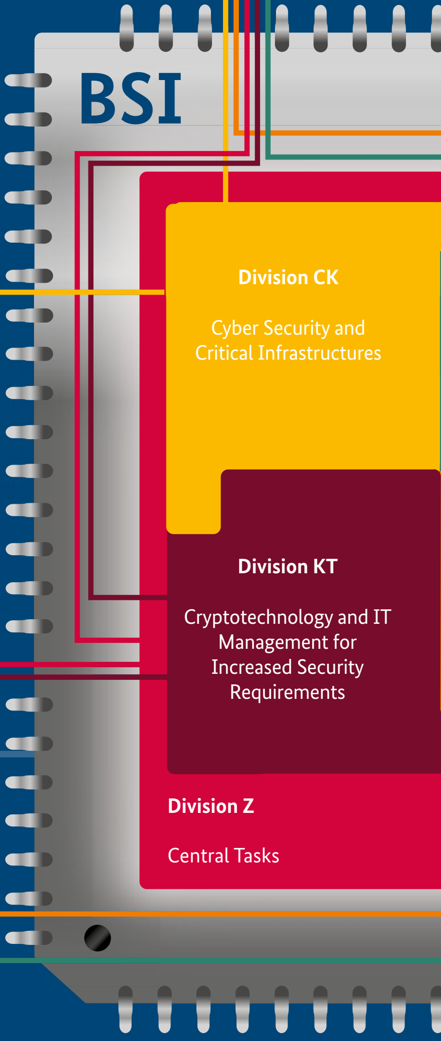
The BSI updates the Strategic situation report and thus shapes prevention of future IT security incidents. The BSI's consultancy services are adapted on this basis to meet the needs of specific target audiences.

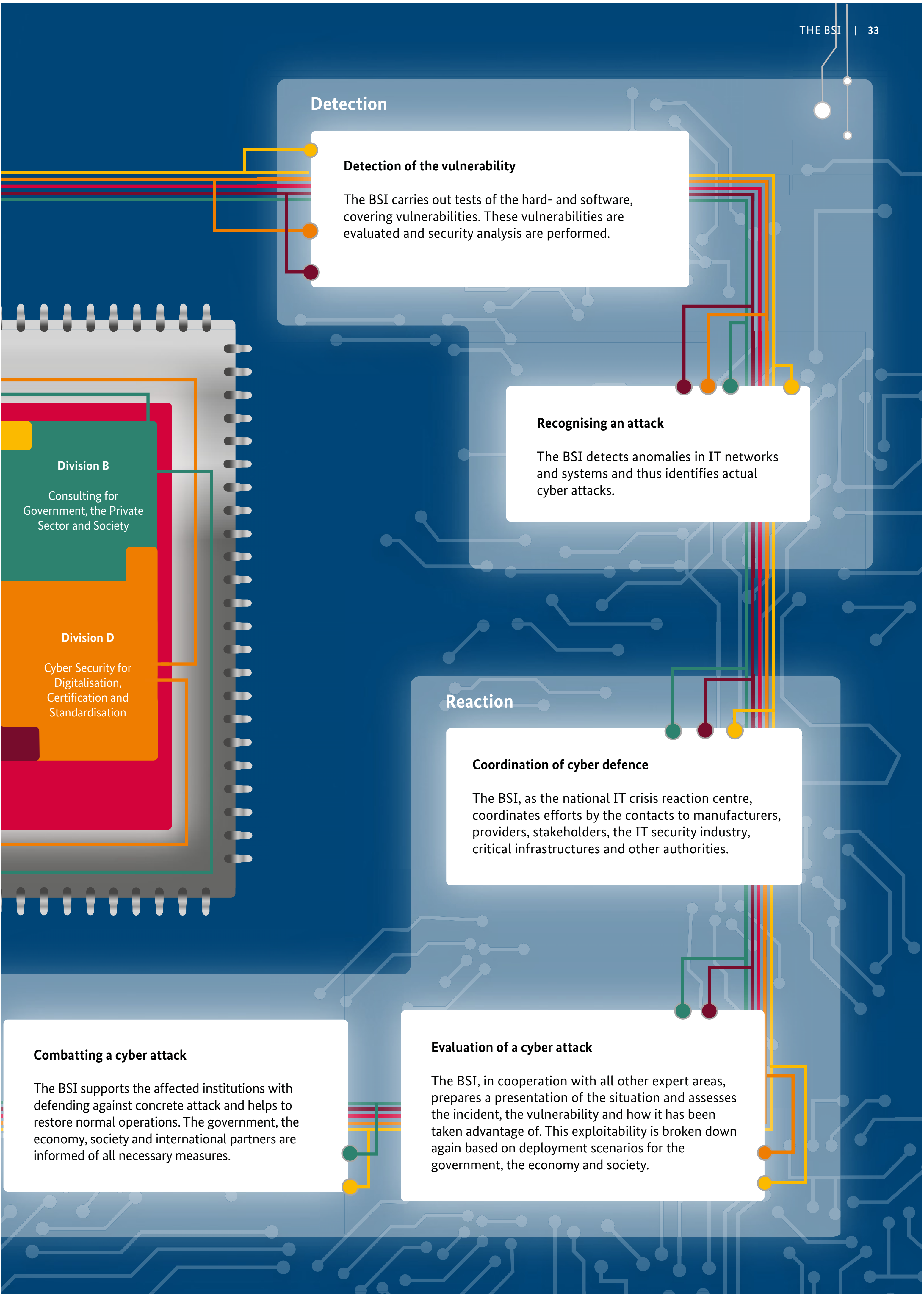
Sustainability

The BSI certification, cryptographic specifications, the BSI's own product developments and penetration tests are adapted and further developed. Where necessary, the BSI makes suggestions on the further development of the legal framework.

Customising specifications and products

The BSI adapts the requirements to the "state of the art" as well as the test structures in a sustainable manner. Furthermore, it constantly improves security technologies and adapts the IT security measures together with the manufacturers.


BSI
Division CK
Cyber Security and Critical Infrastructures
Division KT
Cryptotechnology and IT Management for Increased Security Requirements
Division Z
Central Tasks



Detection

Detection of the vulnerability

The BSI carries out tests of the hard- and software, covering vulnerabilities. These vulnerabilities are evaluated and security analysis are performed.

Recognising an attack

The BSI detects anomalies in IT networks and systems and thus identifies actual cyber attacks.

Division B

Consulting for Government, the Private Sector and Society

Division D

Cyber Security for Digitalisation, Certification and Standardisation

Reaction

Coordination of cyber defence

The BSI, as the national IT crisis reaction centre, coordinates efforts by the contacts to manufacturers, providers, stakeholders, the IT security industry, critical infrastructures and other authorities.

Evaluation of a cyber attack

The BSI, in cooperation with all other expert areas, prepares a presentation of the situation and assesses the incident, the vulnerability and how it has been taken advantage of. This exploitability is broken down again based on deployment scenarios for the government, the economy and society.

Combatting a cyber attack

The BSI supports the affected institutions with defending against concrete attack and helps to restore normal operations. The government, the economy, society and international partners are informed of all necessary measures.

The BSI is Growing with its Tasks

By Dr. Ildiko Knaack, Section Organisation, Yanick Detzel, Section Internal Services, Arno Köster, Project Group for the Realisation of a New Office Building

New Jobs, New Organisation, New Buildings

The BSI as the national information and cyber security authority was further strengthened this year with the allocation of 180 positions. The office thus grew by almost 30 % to now around 850 posts. Managing this growth means, on the one hand, attracting and retaining qualified employees, accommodating them and ensuring their integration. On the other hand, the organisation has also been adapted to perform its new tasks.

ALLOCATION OF POSTS IN 2017

+30%

Das BSI als die nationale Cyber-Sicherheitsbehörde
gestaltet Informationssicherheit in der Digitalisierung
durch Prävention, Detektion und Reaktion
für Staat, Wirtschaft und Gesellschaft

gestaltet Informationssicherheit
durch Prävention, Detektion
für Staat, Wirtschaft und
Bundesamt
für Sicherheit in der
Informationstechnik

Upper left: The new rental property Heinemannstraße, which was occupied in May

Upper right: Festive celebration of the new building

Left: Lord Mayor of Bonn, Ashok Sridharan, and BSI President Arne Schönbohn and his colleagues from the Austrian Federal Ministry of Finance, Wolfgang Ebner, the Swiss ISB, Peter Fischer, and the Luxembourg-based ANSSI, Gerard Caye

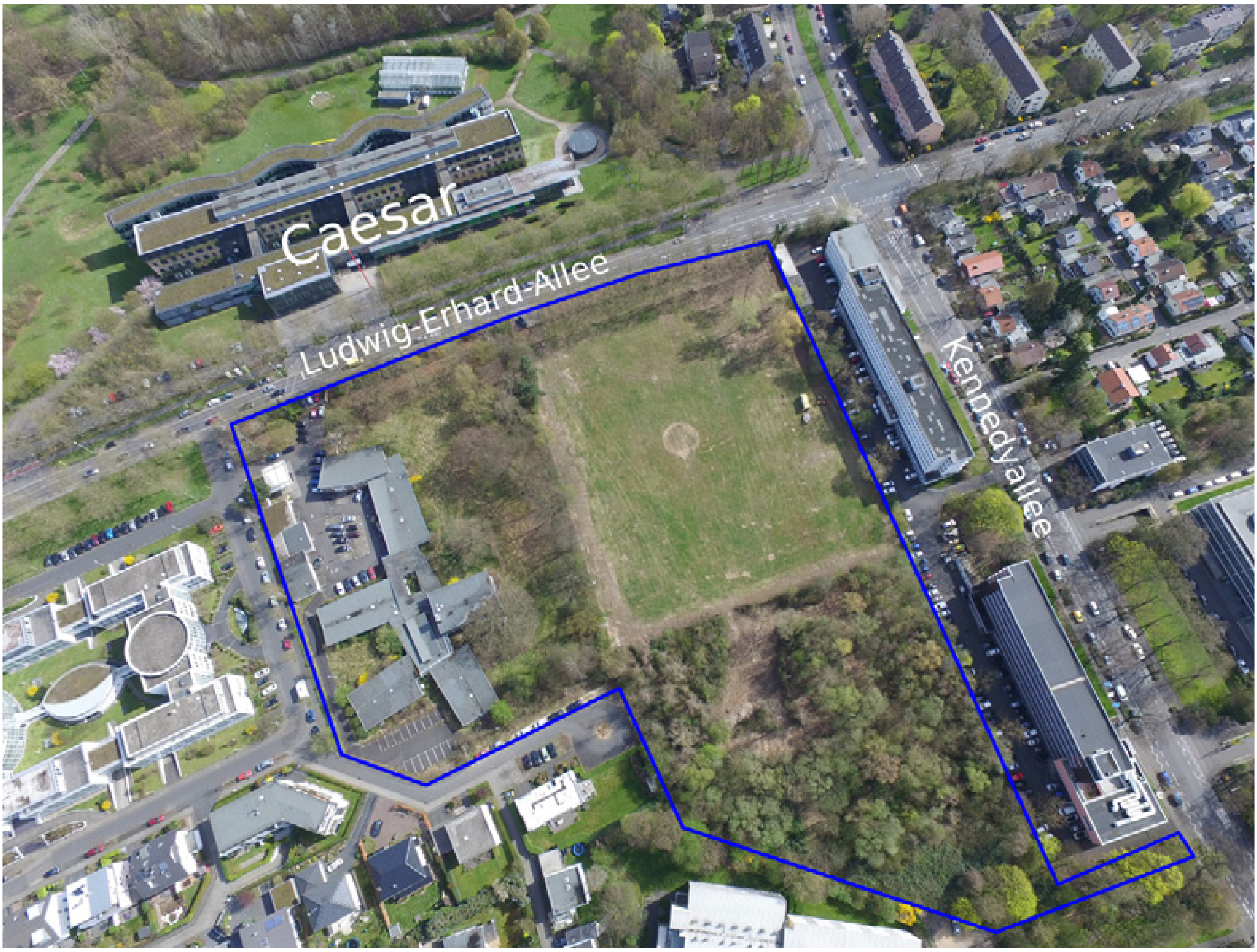
In order to be able to cope with the job growth of the past few years in terms of space, the BSI moved into another rental property in May of this year. The property, which is within easy walking distance from the main building of the BSI, now houses division D and three other sections of division B over two floors. The real estate market in Bonn is currently being re-explored on the basis of the approved space requirements for 2017 to rent yet another property. The aim is to find, with the help of the Institute for Federal Real Estate (BImA), another building that meets the requirements of the BSI and would best be located in the vicinity of the already rented space.

A NEW OFFICE BUILDING

The current separate accommodation in three different properties makes the business processes of the BSI considerably more difficult. In addition, there are unnecessary travel times, as employees have to commute between locations. This unsatisfactory situation is to be ended by a new office building.

This new office building should be located as centrally as possible, not least in order to allow close cooperation with other authorities and large companies, particularly around the former government district. The direct proximity to our partners and the associated immediate availability of know-how are decisive success factors for the task fulfilment of the BSI. A further criterion is our steadily growing task portfolio. It is foreseeable that this will provide for more staff and greater space requirements. This is why the new service property is to be designed in such a way that variable use is possible. Finally, the traffic situation also plays an important role. Due to availability requirements, it is important that the BSI can be easily reached by motor vehicles and public transport at all times.

The BSI as the national cyber security authority will therefore implement an address defining new building at the location in Bonn that meets the BSI's security, confidentiality, technical and functional requirements, reflects the character of the office as an advanced IT



Planning area for the new building of the BSI

security authority, secures optimal support for the authorities' operational processes, provides a positive and up-to-date work environment for employees and allows for expansion options.

Due to availability requirements, it is important that the BSI can be easily reached by motor vehicles and public transport at all times. The planning area is located just one kilometre away from the BSI's current offices on Godesberger Allee in the northern part of the Bad Godesberg district of Plittersdorf, directly opposite the Caesar research centre. The building site owned by the Institute for Federal Real Estate spans approximately 37,500 sqm. The building area is bounded by Ludwig-Erhard-Allee to the northeast, Johanna-Kinkel-Straße to the northwest and west, and borders the existing development along Kennedyallee and Frankenstraße to the south.

Around 950 employees are forecasted in the planning of the new building. On the basis of the defined space programme and the office requirements, about 60,000 sqm of total floor area are required. In order to achieve this, different urban design concepts are conceivable on the property. For the design of the new building, an architectural competition is to be carried out taking into account the urban development conditions of the city of Bonn. The competition result will then be the basis for the further development plan procedure.

REORGANIZATION

At the beginning of 2017, the BSI was reorganised in order to take account of the growing tasks and the associated increase in personnel. The new structure reflects the target groups government, business and society as well as the fields of activity prevention, detection and reaction, in which the BSI is shaping information security in digitalisation. The four specialist departments are supported by the central department. ■

THE FOUR EXPERT DEPARTMENTS AND THE CENTRAL DEPARTMENT

DIVISION CK

In **division CK “Cyber Security and Critical Infrastructures,”** cyber attacks on government networks and federal agencies are detected and cyber security is designed in operating systems, applications and on the Internet around the clock. Penetration tests and IS revisions are also carried out preventively by BSI employees. Furthermore, the department includes the operational National IT Situation Centre, the reporting office for, among other topics, IT security incidents, the Federal Computer Emergency Response Team (CERT-Bund), the National Cyberdefence Centre and the Mobile Incident Response Teams (MIRTs). The daily IT situation report is also created in this department. One additional preventive focus that has been strongly developed with the implementation of the IT Security Act is the support for critical infrastructures. And, last but not least, the well-known BSI IT-Grundschutz is being further developed.

DIVISION B

In **division B “Consulting for the State, the Business World and Society,”** all consultancy tasks are bundled within the scope of prevention. These include classical information security advisory services, prevention of interception and eavesdropping, as well as IT security for IT consolidation, security for government networks, cloud computing, and information security products for authorities. In addition to the government, division B also addresses cyber security issues for companies and society and maintains international relations. Furthermore, national communication is set up with other federal authorities. The implementation and development of IT security standards for politics and professional support for legal issues with IT security reference are also responsibilities of this department.

DIVISION KT

The **division KT “Cryptotechnology and IT Management for Increased Security Requirements”** bundles on the one hand all tasks in the area of the specifications and approvals of cryptographic systems, and is, on the other hand, responsible for their evaluation and operation. These include, for example, VS-IT systems, cryptographic procedures and secure mobile solutions. The emission security of IT devices and systems is also subject to continual testing here. Finally, this department is responsible for crypto and key management. The management, planning and operation of a wide range of IT procedures with increased IT security requirements, as well as the BSI’s own IT security management, are also tasks of this department.

DIVISION D

Cyber security in the digitalisation of government, the business world and society is a focus of **division D “Cyber Security in Digitalisation, Certification and Standardisation”**. Another focus is cyber security for electronic identities (eID) in applications in e-government, chip cards, control infrastructures and assurance of the related chip security. The department is also involved in the design of national, European and international standards and issues the most certificates in the world for hardware-related procedures, software, COTS products and IT security service providers.

DIVISION Z

The **central division Z “Central Tasks”** with the classical task areas of organisation, personnel management, budget and internal services as well as the allocation and project support of more than 150 projects a year and the object and secret protection, which is particularly important for an IT security authority, supports the divisions by providing internal services.

SECURITY NEEDS MEET RISK PREPAREDNESS

15th German IT Security Conference

From 16 – 18 May, the most important representatives of the IT security industry met at the 15th German IT Security Conference in Bonn, which was held under the motto "Digital society between risk preparedness and security needs" this year. Some 600 participants exchanged ideas in the more than 50 expert presentations and panel discussions that were held on topics such as the challenges of digitalisation, the Internet of Things and quantum cryptography. The conference was accompanied by an exhibition that rounded off the discussions.

Das BSI als die nationale Cyber-Sicherheitsbehörde
gestaltet Informationssicherheit in der Digitalisierung
durch Prävention, Detektion und Reaktion
für Staat, Wirtschaft und Gesellschaft

Above: From left: BSI President Arne Schönbohm, Andreas Könen (BMI), Wolfgang Ebner (BMF Austria), Peter Fischer (ISB), Gerard Caye (ANSSI Luxembourg) and Guillaume Poupard (ANSSI France)

Below: Participants in the 15th German IT Security Conference in the Stadthalle Bad-Godesberg in Bonn

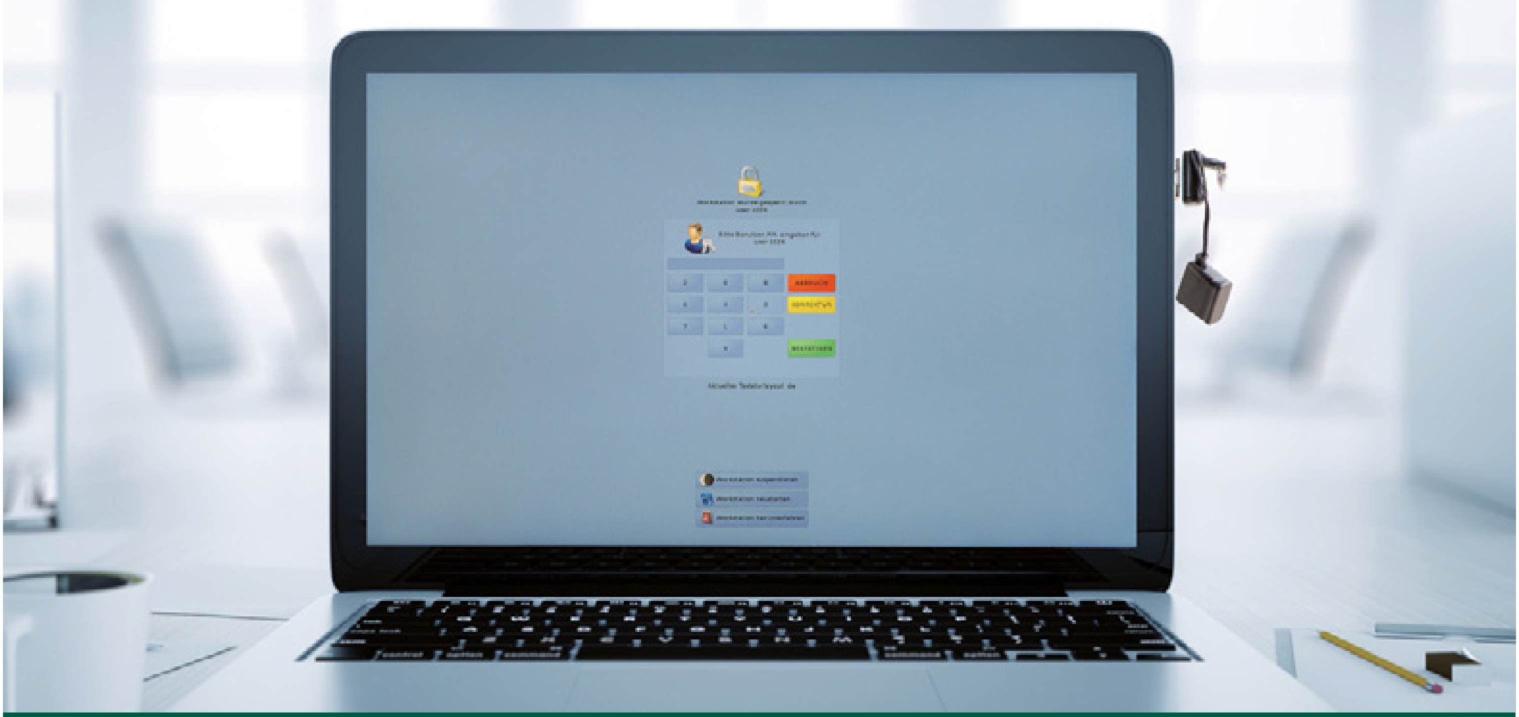
Only days after the cyber-attack involving the ransomware "WannaCry," which affected computers in 150 countries, the topic of cyber threats dominated not only the start of the IT security conference, but again highlighted the importance of cyber security. In his opening speech, BSI President Arne Schönbohm emphasised that the government is not defenceless and cited its ability to act as an important component of IT security. Digitalisation will only be successful if the government can ensure information security. The German IT Security Conference, a permanent event in the IT security industry's calendar every two years, seeks to examine cyber and IT security from different perspectives in order to present and develop forward-looking solutions. ■

IT SECURITY
IN PRACTICE

Confidential, Mobile Working

By Oliver Zendel, Head of Section Cryptography in Applications

Collaborative Processing of Classified Digital Information



Modern IT systems are usually only designed to process classified digital information to a certain degree of secrecy because they are always developed and implemented amid the conflicting interests of functionality, cost, security and time. On the other hand, SINA Workflow, which has been designed according to the requirements of the BSI, meets the demands of an electronic processing system for classified digital information, even for higher secrecy levels.

Who hasn't been in the same situation? Shortly before the end of the work day, important information needs to be written down and distributed to the right addressees as quickly, efficiently and securely as possible. Modern IT systems come with the promise of being able to depict such application scenarios. These systems are generally only designed to process classified information up to the maximum secrecy level RESTRICTED, however. But what if the secrecy level is CONFIDENTIAL or SECRET? The realisation of suitable IT systems for processing digital classified information is implemented in stress field between functionality, cost, safety and time. What if the Federal Republic of Germany or one of its states could be severely harmed by unauthorised access, in certain cases even danger to life and limb?

THE NEED-TO-KNOW PRINCIPLE

In order to minimise this risk, only the parties who need this information to carry out their tasks should be entitled to access classified information. This is called the “need-to-know” principle. In order to implement it in a transparent and verifiable manner, it is a good idea to adopt a rights and role concept based on cryptographic procedures. This means that all protectable information is stored in encrypted form. Only users who are allowed to access the information in accordance with this principle are able to decrypt it. Complementing this encryption with a secure environment to decrypt, encapsulate and view the information provides a secure flow of information.

SECURITY OVER THE COMPLETE LIFE CYCLE

In order to implement these application scenarios, the complete life cycle of classified digital information must be mapped. In particular, the protection objectives of confidentiality, integrity, availability and authenticity must be ensured during the processing of classified digital information over its complete life cycle. This life cycle can generally be described as follows:

- Creation: environment for the controlled creation and processing of classified information with commercial product integration capability
- Storage: software for secure storage of classified digital information
- Access and administration: administration of registry, documents, metadata and indexes for the orderly access to the securely stored information while preserving the “need-to-know” principle
- Process support: workflow and business process management software for controlling the processes of classified information, such as forwarding, registering or printing
- Logging: software for auditing process logging according to legal and regulatory requirements. This creates the necessary audits and records them safely.

Comprehensible administrative action also plays an important role in the processing of classified digital information. Grouping documents into operations and files is an indispensable functional requirement as the basic functionality of transparent administrative action. For the management of classified digital information, in addition to the orderly storage in processes and files, the secure identification of individual documents, processes or files is also important. This secure identification makes it possible to reliably link metadata, particularly the degree of secrecy, to classified digital information.

SECURE AND TRUSTWORTHY VERIFICATIONS

The protection of information that must be kept secret represents a great responsibility for everyone involved. Trust is given to every user. This means that it is technically imperative that decisions made by users be verified. This is performed by way of a function that binds actions securely and demonstrably to users, similar to a signature at the bottom of a contract. These electronic verifications are the reliable basis for the directories required by the regulations, such as the inventory or the receipt book.

WORKING COLLABORATIVELY WITH WORKFLOWS

As a rule, several parties are involved in document creation. There are numerous reasons for this: it sometimes has to do with quality assurance, sometimes with the collaborative creation of texts. One tried and tested process for quality assurance in public authorities is, for example, recording. A modern IT system for the realisation of electronic process treatment of digital classified information has to offer these processes securely. It must therefore be considered that not all users and application scenarios are the same. Workflows must be flexibly adaptable without this necessary flexibility adversely affecting the security features of the overall system.

SINA WORKFLOW

SINA Workflow, designed according to the requirements of the BSI, provides an exemplary implementation of the requirements presented here for electronic process treatment of classified digital information. The Federal Criminal Police Office was gained as a pilot authority during the development of SINA Workflow, testing the solution’s practical relevance in consultation with and with support from the BSI.

For more information see
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/SINA.html

Verification of Digital Certificates

By Dr. Heike Hagemeier and Armin Cordel, Section Requirements for and Development of Cryptographic Mechanisms

Development of a Test Tool as Open Source Software

Digital certificates are an important source of trust for authenticated and encrypted communication. Errors in the validity of these certificates can be of critical importance to security. A BSI project is helping to implement routines for the correct verification of digital certificates.

For digital communication, certificates are needed to confirm the identities of the communication partners or to validate public keys for public key procedures. These digital certificates serve to bind the public keys to the identity of the participants. A participant can be, for example, the server of a bank or another online service.

Digital certificates are managed in public key infrastructures (PKI). A PKI is a certification hierarchy structured like a tree. At the root of this tree is the Root Certification Authority (Root CA). It issues a self-signed certificate, which is then used to sign additional certificates for subordinate certification authorities (Sub CAs). The leaves of the tree are formed by the certificates of the participants. A path from the root to a leaf is called a certificate chain (see figure).

In order for another participant to be able to check the binding of the identity of a participant to his key (or his application), reliable verification of these certificate chains is essential. For example, a browser must be able to verify the identity of the server of a bank using the certificate that is sent by the server. It poses a security risk when invalid certificate strings are accepted by applications (due to programming errors), in the same way as errors in the implementations of cryptographic algorithms.

DIFFERENT FORMATS, MANY ERRORS

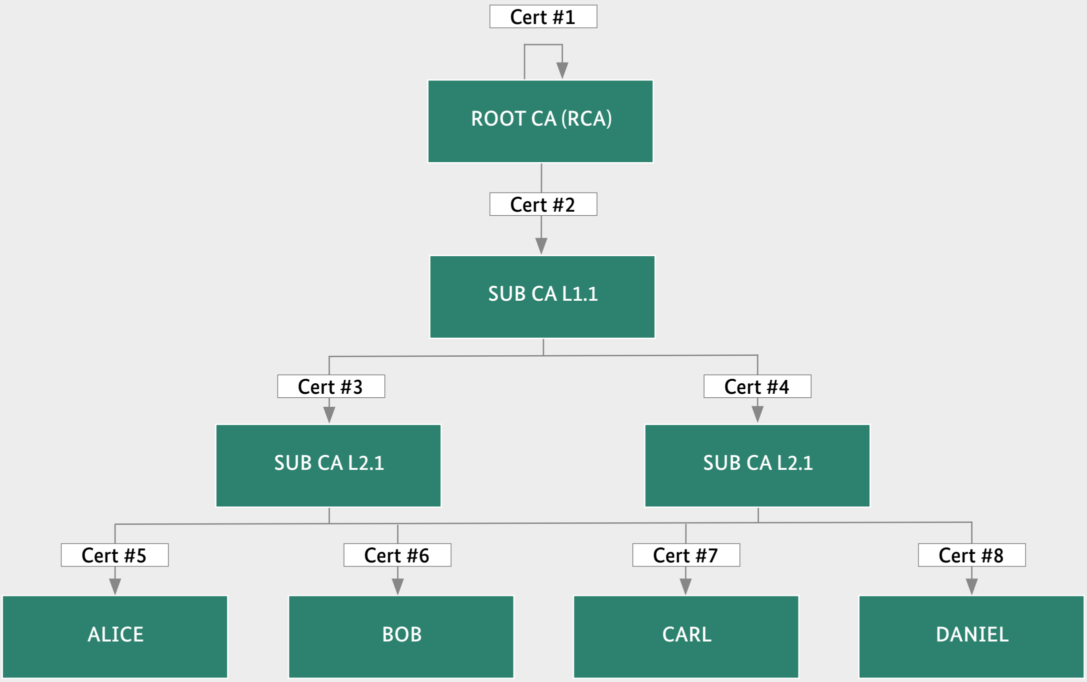
There are different formats for digital certificates, while X.509 (version 3) is the most common standard. This defines a framework for public key infrastructures and digital certificates that can be further specified for the respective fields of application. For the use of X.509 certificates on the Internet, the Internet Engineering Task Force (IETF) has specified concretisations to the X.509 standard in the Request for Comments (RFC) 5280. The format of X.509 certificates with all extensions as well as an algorithm for the verification of certificate chains is described in detail here.

Nevertheless, in the past, errors in the routines for verifying certificate chains have been found in many known crypto-libraries. Researchers at Stanford University and the University of Texas investigated certificate verification in TLS libraries (such as OpenSSL) and libraries for data transport (e.g. Apache HttpClient, cURL) in the fall of 2012 and drew the following conclusion: “Our main conclusion is that SSL certificate validation is completely broken in many critical software applications and libraries.”

Another team of researchers at the University of Texas looked for errors in certificate verification in the most used

EXAMPLE OF A PKI HIERARCHY

The arrows are certificates and the boxes are units / PKI participants



TLS implementations in May 2014. Their approach was to combine new certificates from existing certificates available on the Internet ("Frankencerts"). As a result, they discovered various errors in certificate verification in crypto-libraries such as PolarSSL and GnuTLS.

INNOVATIVE BSI PROJECT

In a BSI project, media transfer AG is currently developing a test tool with the subcontractor cryptosource GmbH that will be able to be used to test routines for the verification of digital certificates or certificate chains. For this purpose, a test specification was developed on the basis of an analysis of RFC 5280 and other relevant standards. The tool creates a series of certificates for every test specification case. Depending on the test case, they form a valid or a faulty certificate chain. Errors are even deliberately installed in certain certificates. For example, the validity period of the certificate may be in the past. By means of these (faulty) certificate chains, (implementation) errors can then be detected in the verification routines.

After completion of the project, the test tool is to be made available as open source. ■

For more information see https://www.bsi.bund.de/VPKI

SECURITY-RELEVANT MODULES

By Jawad Ahmad, Section eID Applications in E-Government and Dr. Astrid Schumacher, Section Director Consulting and Support

TR-RESISCAN and TR-ESOR in Practical Use

Analysing and evaluating security-relevant products and processes in information technology and providing orientation aids and action guides is one of the main tasks of the BSI. In view of advancing digitalisation and the related demand for state-of-the-art and secure e-government solutions, eFile continues to be a main focus as a key element of modernising administrative processes.

TECHNICAL GUIDELINES SERVE AS THE BASIS

As the national cyber security agency, the BSI provides technical guidelines that enable the implementation of corresponding state-of-the-art e-government solutions.

- For legally compliant electronic records management, the BSI-TR 03138 Substitute Scanning (TR-RESISCAN) defines requirements for the proper, risk-minimising design of the scanning process. TR-RESISCAN aims to serve users in administration, justice, business and healthcare as a guide and decision-making aid when it comes to not only scanning but also destroying paper documents after creating the scan product.

- In addition, the BSI defines a guideline for preserving the evidential value of archived data and documents up to the end of the legally prescribed retention obligation with the technical guideline BSI-TR 03125 “Preservation of Evidence of Cryptographically Signed Document” (TR-ESOR) based on the international standards RFC 4998 and RFC 6283 and the ETSI-AdES signature formats as well as the eIDAS regulation and the Trust Services Act.

Legislators are demanding for electronic file management that the “state-of-the-art” (among others, in Sections 6 and 7 of the Promotion of Electronic Government Act (eGovG), as well as in Sections 298a Code of Civil Procedure (ZPO) and 32e Criminal Procedure Code (StPO)). The “state-of-the-art” is regularly complied with when BSI technical guide-lines are followed.

Simulation studies were performed for both the ArchiSig model, on which TR-ESOR is based, as well as for a digitisation produced according to TR-RESISCAN. These have proven in legal terms that the respective evidence value can be optimised and the evidence in court can be simplified accordingly if TR recommendations are followed.

TR-RESISCAN

With its structured requirements, TR-RESISCAN provides pragmatic orientation aids to ensure proper scanning processes. Due to the modular structure, a concept tailored to one’s own application is possible, which, in addition to pre-serving the probative value of the paper-bound original (e.g. in court), also takes an appropriate cost-benefit ratio into account. All basic security requirements for integrity, confidentiality, availability and data protection are already met with the basic module.

The practical implementation of TR-RESISCAN has already been carried out by numerous users in the areas of administration and business. Among other things, the guideline for replacing scanning of documents in municipalities was developed. Hubert Ludwig, Managing Director of DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH, explains the benefits of TR-RESISCAN:

> *“The technical guideline TR 03138 Replacing Scanning (RESISCAN) of the BSI is an important supporting instrument for the advancing digitalisation. Depending on the need to protect the documents, more legal certainty can be obtained for the scanning process if the paper is to be destroyed after scanning and only the digital document is to be used. Accordingly, certification is an important proof that the processes and systems for replacing scanning meet the technical and organisational requirements set out in the Directive.“*

For Torsten Wunderlich, head of the DATEV information office in Berlin, TR RESISCAN has long proven its value in practice:

> *“The combination of an industry-specific procedure description and BSI-RESISCAN certification ensures the maximum value of proof during the replacement scan, as a legal simulation study has demonstrated. The tax consultants have set a standard with their sample procedure description that serves as a role model for other sectors and motivated the DATEV solution.“*

TR-ESOR

TR-ESOR describes a possible reference architecture of a system for the evidence and information preservation of electronic documents with requirements derived therefrom on the basis of international, European and national standards.

The TR-ESOR Technical Directive deals with the topics:

- Data and document formats,
- Exchange formats for archive data objects and proof data,
- Recommendations on a reference architecture, its processes, modules and interfaces as a concept of a middle-ware,
- Additional requirements for federal authorities as well as
- Conformity rules for conformity level 1 “functional conformity,” conformity level 2 “technical conformity” and conformity level 3 “Conformity with the German federal authority profile.”

In addition, TR-ESOR products can be certified according to the Common Criteria Protection Profile BSI-CC-PP-0049-2014.

The Technical Guideline TR-ESOR derives a modular reference architecture from the functional requirements for the preservation of the probative value. On the basis of the present requirements catalogue, vendors and product manufac-turers can develop compliant solutions for the directive 03125, which can be certified on the basis of the above-mentioned conformity levels.

OUTLOOK

In particular, the eFile, which is anchored in law for the public as well as for the administration of justice, is focusing even more on the topics of “replacing scanning” and “long-term storage.” The offer for certification, which applies to both directives, is being perceived not only in the economy, but increasingly also in the public sector. Currently, a total of nine BSI certifications have been carried out according to TR-RESISCAN and four according to TR-ESOR.

The security-relevant modules of the eFile are continually updated in order to stand up to the future challenges of digi-talisation. TR-RESISCAN is currently being revised, together with all of its annexes. In addition to the legal changes, the update also takes into account the feedback from actual practice. From 2018, a revision of TR-ESOR is also planned. ■

For more information see

TR-ESOR
tresor@bsi.bund.de

TR-RESISCAN
resiscan@bsi.bund.de

ZERTIFIZIERUNG
zertifizierung-tr@bsi.bund.de

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

"We Must Take Action"

Interview with Norbert Winkeljohann and Derk Fischer, PwC Deutschland

The fear of cyber attacks is growing. Norbert Winkeljohann, Spokesman for the Management of PwC Deutschland, and Derk Fischer, who is responsible for Cyber Security at PwC Deutschland, discuss how vulnerable digital society is and how the IT Security Act (IT-SiG) makes Germany a safer business location.

■ The world is getting more digital. Everything that can be connected will be. How vulnerable is our digital society?

Norbert Winkeljohann: With advancing digitalisation and increasing connectivity, areas vulnerable to hacker attack are growing as fast as the many technical possibilities we are benefiting from. Web-based attackers have flexible, high-performance means and are well connected. This is how they spy out information, sabotage processes and paralyse production lines. A primary reason for concern is the attempt to influence democratic elections, as happened in France and the US. However, industrial plants and company IT systems are more often in the sights of the attackers. Successful attacks cause enormous damage. This shows how vulnerable we are. We must take action.

■ How well are companies currently set up to adequately address this issue?

Norbert Winkeljohann: In large corporations, cyber security is promoted by supervisory bodies. However, German family-run businesses and SMEs are often less secured. Attackers, however, do not distinguish between large corporations and SMEs. At the same time, small and medium-sized enterprises are just as committed to digitalisation: they are transforming their processes and networking with suppliers, business partners and customers. This creates integrated process chains based on highly complex IT infrastructures that present completely new challenges to security. At the same time, attack methods are becoming more aggressive, sophisticated and comprehensive. As a result, cyber attacks are increasing in numbers with steadily rising success rates.

■ Don't SMEs recognize the threat?

Derk Fischer: Regardless of the massive increase in attacks, many smaller companies are reluctant to react with concrete measures. Despite the threat, companies regard themselves as well or very well protected in terms of their own security. However, this self-assess-ment is often based on a traditional process and IT understanding of the decision-makers and does not adequately take current and urgent issues of digitalisation into consideration. There is a gap between self-estimation and the actual threat situation. There is no fundamental problem of not knowing, but a problem implementing changes in the face of transformation challenges.

Profile in brief:

WP / StB Prof. Dr. Norbert Winkeljohann has been the Chairman of the Board of Directors since July 2010, resp. Managing Director of PwC Deutschland and Chairman of PwC Europe. He is also a member of the five-member Executive Board of the global PwC network.

Derk Fischer is a partner in the field of Risk Assurance Solutions. For 26 years he has been in IT security consulting, including 17 years at PwC.

■ The IT Security Act (IT-SiG) has been in force since 2015. Have we seen any initial successes?

Norbert Winkeljohann: Yes, it has had a positive effect. The impetus for action for operators of critical infrastructures (KRITIS) extends far beyond the companies covered by the law. Business partners also need to upgrade if they want to be on the same level in terms of security. Companies are starting to recognise that this pressure is good for them.

Derk Fischer: The IT-SiG ensures that general minimum standards for information security are adhered to, contributing to a striking improvement in information security in Germany. But this should not blind us to the fact that there is still a need to catch up.

■ Where exactly do you see a need to catch up?

Derk Fischer: The act explicitly excludes the public sector, where the legal requirements for preventive measures are lower than for companies. As a result, the public sector has invested less in security than banks or insurance companies, for example.

■ And what will our IT security landscape look like when robots have conquered the operating room?

Derk Fischer: We're currently witnessing an evolutionary leap, the consequences of which we can't yet fully estimate. New self-learning systems are being used, and not only in medicine. There are also the examples of TESLA, BMW, Mercedes and Volkswagen in the automotive industry. Autonomous driving is well advanced here and is only being delayed by missing legal frameworks. For us in society, this means we have to discuss the way we deal with the most personal data behind these topics. Who owns the data, who is allowed to use it and under which conditions? How can we protect it? This requires a balancing act between reaping their benefits and total monitoring. As a society, we need to be in agreement about the basic principles of dealing with the new data world, since politics must also be involved. Threats with criminal intent seem almost secondary to such a claim, even if we have to assume that we will have to deal with these much more than before. ■

PricewaterhouseCoopers (PwC) is an auditing and consulting company based in Frankfurt/Main. On behalf of the BSI, PwC has developed minimum requirements for cloud providers to be examined since January 2016.

For more information see https://www.pwc.de/de/mittelstand/informationssicherheit-im-deutschen-mittelstand.html

“Without Cooperation, You Won’t Get Very Far”

Interview with Dr. Evi Haberberger, LKA Bayern

The Bavarian Criminal Police Office set up Department 54 – Cybercrime in early 2014 to strengthen the Bavarian Police in their fight against Internet crime and to establish a competence centre. BSI Magazine spoke with Dr. Evi Haberberger, Area Director Center Cybercrime, department 54.

Profile in brief:

Dr. Evi Haberberger was born in Bayreuth, Germany, in 1973. After receiving her degree in mathematics from the University of Bayreuth, she earned her doctorate there in discrete mathematics in 2002. From 2002 to 2009, she was responsible for criminal analysis at the Office for Organized Crime in the police department of Oberfranken in Bayreuth, Germany. Afterwards, she joined the Bavarian State Criminal Police Office as a clerk. Since 2014, she has been the Area Director responsible for the SG 541 Centre for Cybercrime at the Bavarian State Criminal Police Office.

■ Dr. Haberberger, what are the aims of the Bavarian Criminal Police Office with respect to the establishment of the cybercrime competence centre?

The main focus of our activities is, of course, the direct fight against all types of cybercrime. But, the networking of colleagues working in the very dynamic field of cybercrime is also very important, as the whole police force is affected by this new kind of crime. And we want to build up expert knowledge and security at various levels: from the officers in training through the investigators in registered offenses involving drugs, weapons, fraud, state protection, etc. to prevention officials and managers.

■ Will the entire cybercrime expertise of the Bavarian police be concentrated in the centre?

No. Bavaria has taken an interesting route with respect to the staff of the Bavarian police, since more and more computer scientists have been recruited and trained as law enforcement officers across the state since 2011. There are currently around 50 officials in Bavaria. In the course of the year 2017, around 70 additional computer scientists will be employed and trained as IT criminalists. As a result, the IT know-how in the Bavarian police force is significantly increasing, since the cooperation of computer scientists and the criminal police is very beneficial for both parties.

■ How is the competence centre organised?

It is a department with currently around 50 employees and consists of three areas: the cybercrime centre, the cybercrime investigations field and the network investigations field. The cybercrime centre also includes the central contact point for cybercrime (ZAC) for authorities and companies.

■ Has the competence centre been completely restructured?

Not completely. The core area was the network investigations field: a precursor field had already been involved with searches on the Internet and with investigation support for the Bavarian police services since 1995. From the outset, one focus was on research on child pornography material on the Internet as well as support for handling these offenses. However, more and more tasks have been taken on over the years in different areas of crime. Cybercrime became almost omnipresent through widespread digitisation and the increasing use of digital information and communication media and technologies. As a result, the personnel increase and department founding were necessary in Bavaria as well.

■ How is the department linked to the LKA?

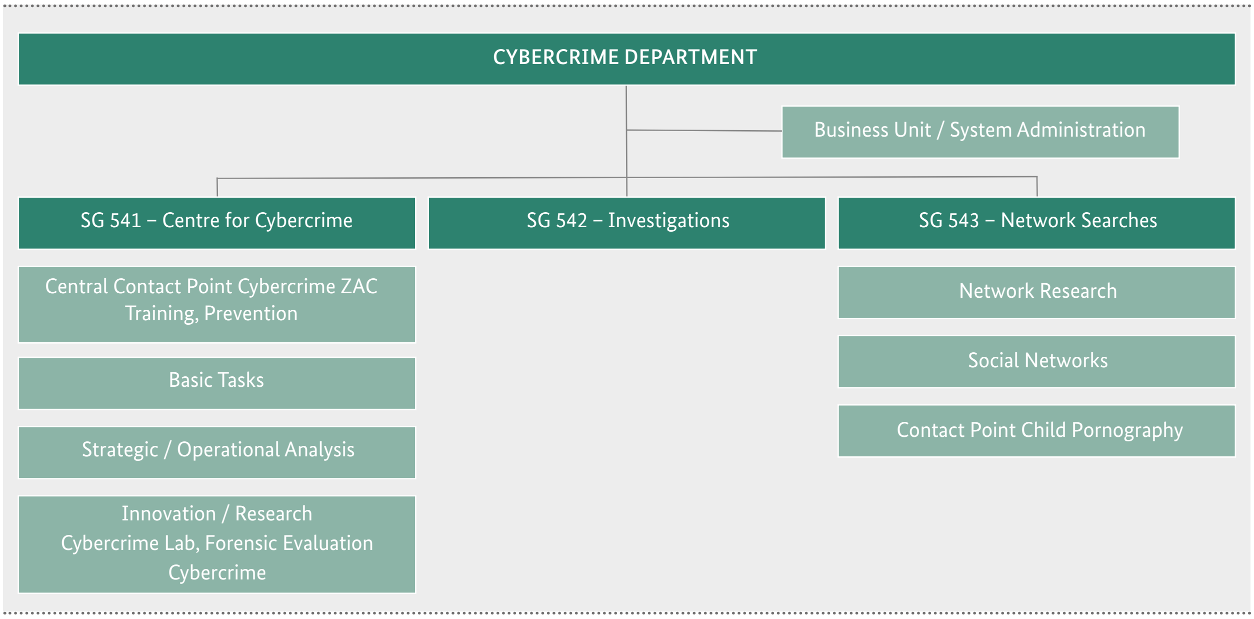
It is based in Department V – Central Criminal Police Services. This underscores the focus and high priority of the support services for the departments of the Bavarian police on cybercrime as their centre point. The competence centre also carries out its own investigations, which are assigned to us by the Bavarian Ministry of the Interior or by the public prosecutor,

> *“It is particularly important to continuously exchange information with the BSI.”*

when a critical infrastructure or an authority is affected by a cybercrime offense, for example. However, an important part is also coordinating nationwide procedures, advising police officers, developing and implementing training and continuing education measures for various target audiences in the Bavarian police, in cooperation with the Bavarian Police Institute, as well as exchanging information with investigators and services on national and federal levels as well as internationally.

How does this information exchange take place?
Well, a good example is an information portal on the Intranet of the Bavarian police, which contains the most important phenomena in cybercrime as well as up-to-date news, investigations and information on contacts and links to audited external sources.

You have addressed the cooperation at the state and federal levels. Can you give us examples of this?
First of all, I would like to emphasize in general that the cooperation with other cyber security players, especially with the BSI as well as the newly emerging cyber cluster at the Bundeswehr University in Munich is extremely important for us as well as for the German police forces as a whole. It is particularly important to continuously exchange information with the BSI. For one, with regard to general technical information, which serves as a source for prevention tips for Bavarian citizens and companies (keyword: BSI for citizens), for another, with regard to the protection of critical infrastructures as a point of contact for our cybercrime centre, which contacts companies in the run-up to possible attacks to be able to act quickly in the event of damage and initiate investigations.



CYBERCRIME DEPARTMENT

Business Unit / System Administration

SG 541 – Centre for Cybercrime

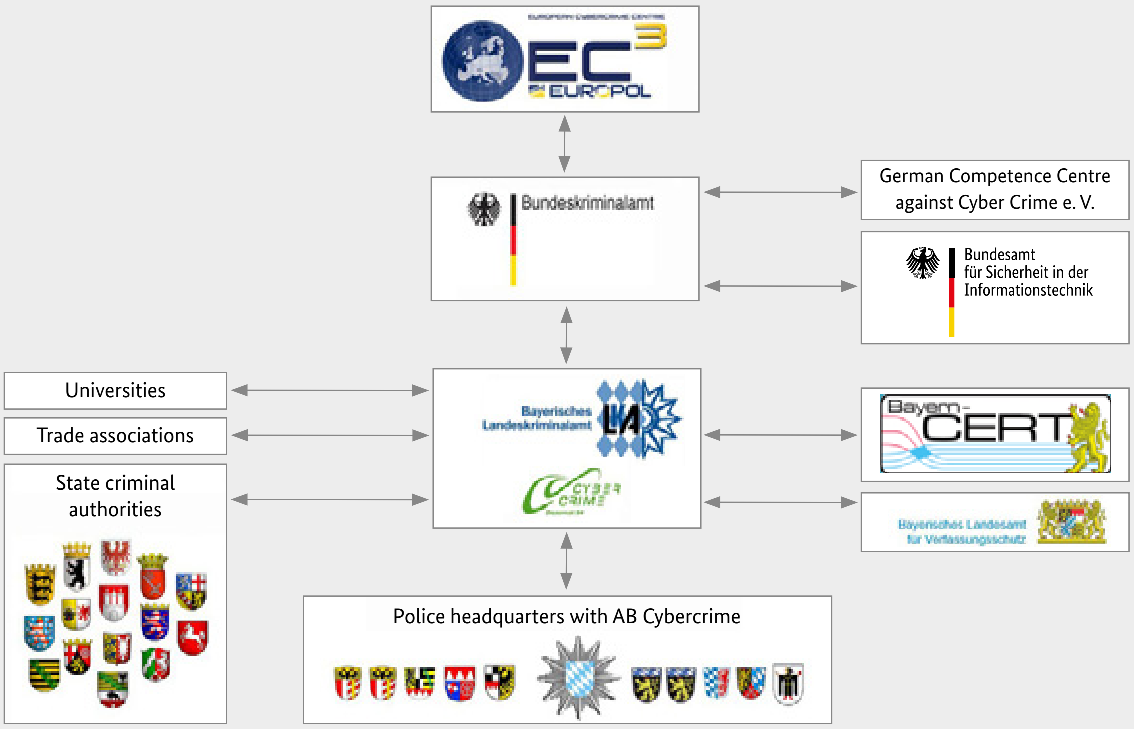
- Central Contact Point Cybercrime ZAC Training, Prevention
- Basic Tasks
- Strategic / Operational Analysis
- Innovation / Research Cybercrime Lab, Forensic Evaluation Cybercrime

SG 542 – Investigations

SG 543 – Network Searches

- Network Research
- Social Networks
- Contact Point Child Pornography

NETWORKING OF DEPARTMENT 54


EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL
Bundeskriminalamt
German Competence Centre against Cyber Crime e. V.
Bundesamt für Sicherheit in der Informationstechnik
Universities
Trade associations
State criminal authorities
Bayerisches Landeskriminalamt
LKA
CYBER CRIME
Bayern-CERT
Bayerisches Landesamt für Verfassungsschutz
Police headquarters with AB Cybercrime

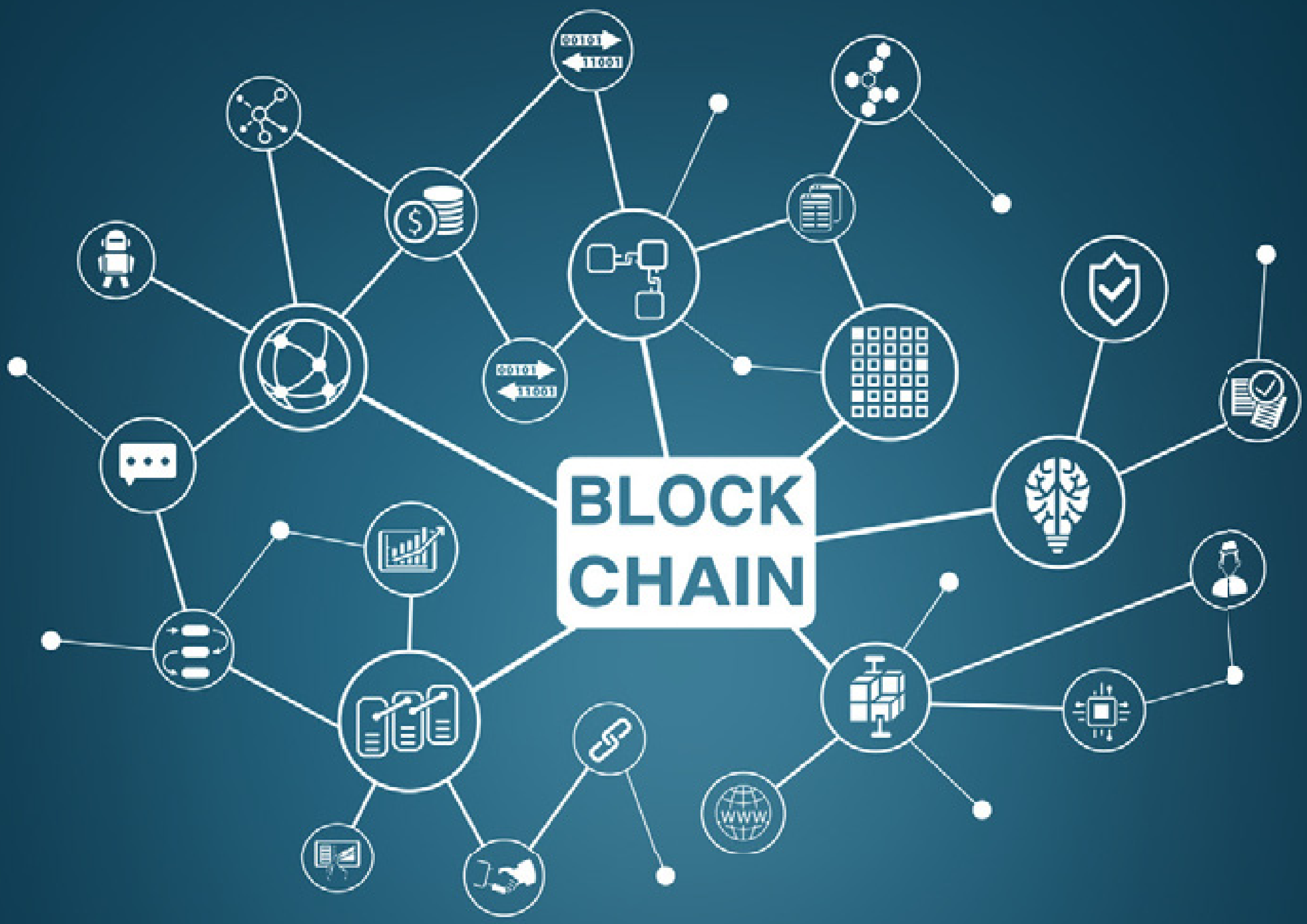
■ Why are these contacts and routines so important?

For the course of investigation, it is essential to identify the attack vectors as quickly as possible and to secure evidence so that follow-up measures can be taken promptly and recovery measures can be taken in the affected companies as early as possible without destroying too many traces of the offenders. In this case, the police's ability to react paired with professional competence, and supplemented with the know-how of the BSI, if needed, is crucial for fighting cyber-attacks.

In addition, inter-departmental contacts are necessary, since it's often not clear at the beginning of an attack, on the energy supply for instance, whether it is a "normal" blackmail cybercrime offense, an act of violent subversion or possibly an attack with an official mandate. Combat and response strategies and mechanisms must be coordinated and jointly developed across the boundaries of competence. It is therefore extremely important for us as an actor in a large network to further develop and maintain this network in order to achieve the best possible protection for our citizens and companies. Cyber security affects us all and can only be managed as a common governmental responsibility. ■

For more information see http://www.polizei.bayern.de/lka/kriminalitaet/internet/index.html

DIGITAL SOCIETY



POTENTIALS AND CHALLENGES OF BLOCKCHAIN TECHNOLOGY

By Dr. Sarah Maßberg and Dr. Manfred Lochter, Section Requirements for and Development of Cryptographic Mechanisms

Cryptographic Mechanisms Create Trust

For several years, virtual currencies such as bitcoin have been in the public eye. Their technological base, Distributed Ledger Technology (DLT), is slowly gaining greater public attention. The blockchain technology discussed in the following article is a special design of DLT based on the virtual currency bitcoin.

"Blackmail with 'Wanna Cry' – Bitcoin fulfils its dubious reputation," was the headline of an article published in the Neue Zürcher Zeitung in May 2017 after a new wave of ransomware beset tens of thousands of computers worldwide. Besides celebratory reports of price peaks for the bitcoin crypto-currency, with 150 % growth in the first half of 2017, there are constant press reports on criminal activities in the bitcoin system that influence the public perception of crypto-currencies and blockchain technology. There is a massive lack of conceptual clarity that sometimes leads to indiscriminate praise of blockchain or to general criticism of the new technology.

TRUST THROUGH CRYPTOGRAPHIC MECHANISMS

The basic idea behind blockchain technology comes from Distributed Ledger Technology (DLT).

WHAT IS A DISTRIBUTED LEDGER?

A distributed ledger is a public ledger with decentralised management. It is the technological foundation of virtual currencies and serves to record transactions from user to user in digital payment and business transactions without the need for a central administration authority to legitimate each individual transaction. A blockchain is a dedicated distributed ledger, and underlies the virtual currency bitcoin for instance.

In a distributed ledger, data is not held centrally but distributed synchronously and consensually. A peer-to-peer network and a consensus mechanism guarantee valid data distribution over all network nodes. In blockchain technology, the distributed consensus is realised by securely linking data blocks.

The actual term "blockchain" was first used for the data structure the crypto-currency bitcoin is based on. But today it has much broader application. The new trust model is common to all blockchain approaches: trust in the integrity and security of data storage does not arise from trust in a central instance, but is based on cryptographic mechanisms such as hash functions and signatures. The rules of the system are encoded intrinsically by chain code (also called smart contracts) and executed automatically.

VARIOUS APPLICATIONS

Various applications can be realised based on blockchain technology. Blockchain, for example, enables automation of the management of insurance claims by accident and damage insurers by quickly assessing claims based on historical events. In the financial sector, there are approaches to making aftermarket trading more cost-effective and faster through the use of blockchains. In addition, blockchain offers the possibility to allow a large part of the world's population, which to this point has had no access to classical financial systems, to participate in trade and business processes (financial inclusion). When granting syndicated loans, blockchain can speed up the formation of the consortium and payment.

The energy industry is also showing increased interest in the new technology. In the field of e-mobility, for example, there are many conceivable application possibilities, such as the processing and payment of charging operations at power stations via a blockchain. In energy trade, there are initial approaches for local blockchain networks in which even small energy producers such as private households with a solar system on the roof can trade their electricity. In the health sector, potential applications are discussed from electronic healthcare via digital health insurance up to drug safety.

State approaches to blockchain technology exist as well. Different countries (e.g. Ghana and Sweden) are experimenting with blockchain-based digital land registries. The distribution of UN assistance funds in Jordan was recently implemented through a blockchain solution. And Estonia, the pioneer of digitalisation in Europe, has already used blockchain technology in various areas such as the e-residency program, transnational digital citizenship and the management of health data.

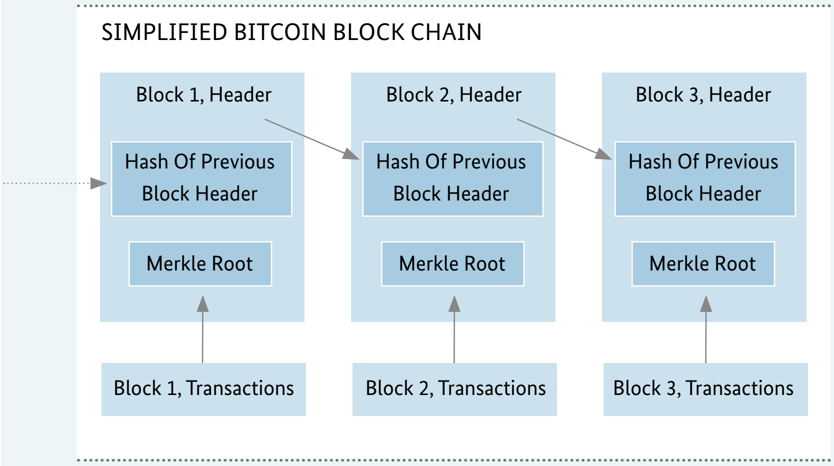
A PROMINENT EXAMPLE: THE CRYPTO-CURRENCY BITCOIN

A particularly prominent application of blockchain techno-logy is crypto-currency, a digital means of payment with a distributed, decentralised and cryptographically secured payment system. And bitcoin, in turn, is a special case – the most successful example of a crypto-currency so far.

Transactions (payments with bitcoin) are authenticated in the bitcoin system using a public key method. On the one hand, cryptographic keys are used to address payment recipients (public keys) and, on the other hand, to sign the transactions by the senders (secret keys).

The transactions are distributed in the bitcoin network and then merged into new blocks by so-called miners and attached to the end of the bitcoin blockchain. This attachment (see figure) is secured using a cryptographic hash function. This ensures the integrity of the entire chain.

SIMPLIFIED BITCOIN BLOCK CHAIN



In order to add a block, a CPU-intensive task (a crypto-puzzle) must be solved. If the miners solve this task and extend the blockchain, they are rewarded in the form of bitcoins and can expect additional transaction fees. This process, also known as proof-of-work (PoW) or mining, is the consensus mechanism in the bitcoin system.

A serious drawback of bitcoin is the limited data throughput in the bitcoin network and the tremendously high energy consumption due to the required computing power of mining. It currently represents roughly the entire power of a conventional power plant.

Even though the cryptographic mechanisms used today are considered safe, the question of implementation security remains. This concerns bitcoin software and the security of bitcoin “wallets,” in which cryptographic keys are managed. Cases have arisen in which key generation was very weak and permitted theft. Bitcoin also has an open developer community, which is difficult to observe and control.

It is often argued that the bitcoin system guarantees anonymity since participants are addressed only via a cryptographic key (and thus a random bit sequence). However, successful attempts have been made to identify owners of bitcoins by the collection and analysis of metadata. On the other hand, bitcoin’s promise of anonymity is very attractive to criminals. Bitcoin has become a popular hacker currency and the standard payment tool on the Darknet, as recent ransomware blackmail attempts show.

STANDARDISATION BEGINS

In April 2017, TC 307 “Blockchain and Distributed Ledger Technologies” was set up at the International Organisation for Standardization (ISO) under the leadership of Australia to set new technology in a certain formal framework, to define terms and to lay the foundations for regulatory measures. This brought the first international standard on blockchain into being.

In addition, associations in industry (e.g. R3 Consortium, Hyperledger Project) are developing quasi-standards for different business sectors that have a major influence on the development and use of blockchain. Furthermore, many research institutes (such as the Fraunhofer Society) and business associations (e.g. Bitkom and Teletrust) have already dealt intensively with the subject and published relevant papers and statements.

PROBLEMS AND CHALLENGES OF BLOCKCHAIN

Many of the problems of blockchain technology encountered in practice have not yet been solved. Since the security of blockchain technology is largely cryptographically based, the selection and implementation of the cryptographic primitives and protocols used plays a major role. Even during system design, long-term security should be noted, e.g. in the form of changing mechanisms.

The other known problem areas of IT security such as endpoint security, network security, hardware and software security have also not yet been solved in blockchains, and are a major challenge in distributed, decentralised systems that has not yet received sufficient attention.

WHAT IS BITCOIN?

Bitcoin (“digital coin”) is a worldwide usable decentralised payment system and the name of a digital money unit. The system was first described in 2008 in a white paper published under the pseudonym Satoshi Nakamoto. The following year, an open source reference software was released. Nakamoto also created the first block (genesis block) of the bitcoin blockchain and with it the first 50 bitcoins. It is still unclear what person or group hides behind this name as Nakamoto’s bitcoins have not yet been used.

There is also a great deal of uncertainty regarding legal questions concerning the use of blockchain. The terms used in legal texts today often do not fit into the technological content and need to be interpreted in context first. The lack of a central authority can be a problem. Particularly in data protection, there are still reservations towards blockchain technology, as some basic principles such as data economy or the right to be forgotten appear to contradict the construction of a blockchain.

The possibility of connecting participants transnationally is also a challenge. For many, blockchain applications require a certain degree of internationally coordinated control and regulation – even in a decentralised, distributed system. If a blockchain is operated across national boundaries, the question will need to be answered as to who is responsible for its regulation and corresponding enforcement.

SHAPING REQUIRED

Today, the word “hype” often comes up when discussing the economic and organisational advantages of blockchain technology. Regardless of whether or not blockchain is overrated, it should be expected that a number of applications using it will remain in wide circulation.

Blockchains offer huge potential, especially in applications where a non-transparent central authority is undesirable, or where digital infrastructures have so far not been adequately implemented. The use of blockchain technology could also promote the transparency and cooperation of government authorities in government applications.

The BSI as a shaper of IT security in Germany deals intensively with the security aspects of blockchain against the backdrop of possible applications in government or critical infrastructures and the threats of criminal activities in blockchain networks.

In order to be able to capitalise on the opportunities of blockchain technology and to control the risks, further efforts are definitely required in the area of standardisation and regulation to ensure that blockchain’s trust model can withstand the requirements of legally secure, real-world applications. Besides this, the use of strong cryptography and secure protocols should be ensured for all applications. This applies in particular to applications that store confidential (e.g. personal) data in a blockchain. Data confidentiality and integrity must be cryptographically secured for the long term. Long-term security is a very challenging goal when considering the simultaneous discussion of potential quantum computing (see BSI Magazine 2017/01), which would endanger parts of cryptography in use today. ■

For more information see https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Benutzerdefinierte_BS/BS_Bitcoin.html?nn=7712584

25 Years of genua

By Dr. Magnus Harlander, Managing Director of genua gmbh

Working in Partnership with the BSI

Profile in brief:

Dr. Magnus Harlander, as Technical Managing Director of genua gmbh, is responsible for the development of security solutions as well as the certification of high-quality products in cooperation with the BSI. The physicist founded genua, based near Munich in Kirchheim, Germany, in 1992 together with two other IT security specialists.

> *“Participation in a research project on high-performance firewalls, sponsored by the BSI, was a decisive turn for product development.”*

The company genua is celebrating its 25th anniversary this year. Since its founding in 1992, many things have happened in the field of IT security: while viruses circulating online like “Michelangelo” and “I Love You” were still known by name, today more than 390,000 new malicious programs are registered on the Internet every day. Hackers used to be for the most part playful techies, but today they are mostly members of professional organisations. In the industry too, there have always been highs and lows and bursting bubbles. In its 25 years of rapid development, genua has developed from the spin-off of three physicists from the Technical University of Munich into an important provider of high-quality IT security in Germany. The BSI, founded in 1991 and thus almost the same age, was a constant companion during these years. As both the BSI and genua pursue the goal of advancing IT security in Germany, the two partners have joined forces to create a constructive partnership.

A very important step for genua was the BSI certification of their genugate firewall in March 2002 according to the standard ITSEC. genugate was the first firewall to receive a BSI certificate. The entire process, begun in 1998, resulted in a certificate that independently certified the high security level of the solution.

BSI CERTIFICATE OPENS DOORS

For genua, BSI certification turned out to be the door-opener to high-security firewall projects. For instance, in 2002, the tender for securing the large government network IVBB was won, as genugate had proven to fulfil both its high functional and security requirements. genugate is still in use in this central network – as of today, without a single failure. As we can see, BSI certification keeps its promises.

Numerous other firewall projects in government and the industry sector followed. New versions of genugate have been regularly re-certified at the BSI according to the currently used Common Criteria procedure.

genua also regularly cooperates with the BSI on approving IT security solutions for classified data processing. In April 2017, we received admission for the secrecy level VS-NfD for the security laptop vs-top. With this user-friendly solution, mobile employees can safely connect to classified networks.

However, it should also be noted that the authorisation procedure for the security laptop based on microcore technology took about two and a half years. Both in the interest of manufacturers and users, procedures should be accelerated to ensure that this market can be supplied with a choice of current solutions. genua has been intensively involved in the talks to accelerate approval and certification procedures at the BSI, and good results have been achieved.

IMPULSES FOR PRODUCT DEVELOPMENT

genua has always received important impulses for product development from the BSI. In the design of their two-stage firewall, for example, the company followed the BSI recommendation that three-level security systems should be used at critical interfaces. genugate consisted of a combination of an application level gateway and a packet filter and thus already offered two levels. If an additional firewall were added, the recommended solution would be reached. The two-stage system is a central security feature and is thus predestined for use in the high-security area.

BSI specifications have also been implemented in the development of genucard, the personal security device for the secure connection of mobile employees and home offices: the compact device is used by many public authorities and organisations that perform security tasks, allowing, among others, the German Federal Armed Forces to set up secure home workplaces.

Participation in a research project on high-performance firewalls, sponsored by the BSI, was a decisive turn for product development. Again, genua took on microcore technology, recognising its advantages: the minimalist operating system is a flexible platform for developing solutions that meet the highest safety requirements. The first products with this technology are security laptops for mobile users dealing with classified information and data diodes for monitoring critical infrastructures.

It is easy to see that the BSI had a helping hand in genua's successful development. The company is keen to carry on this good cooperation and hopes that the BSI will continue to provide important impulses for the industry, to specify demanding security standards and to assert itself in all critical areas. Vendors are able to translate the required standards into products and have the opportunity to prove the quality of their solutions through appropriate approval and certification procedures. In this way, all together, the industry can continue to advance IT security for the next 25 years.

For more information see https://www.genua.de

SMART AND SECURE

By Hanna Heuer, Section Cyber Security for Citizens; Public Relations, and Florian Schumacher, Section Cyber Security for Society

Project "Digital Society" Nearing Completion

"Digital Society: Smart and Secure." Under this motto, representatives from civil society, the sciences, the commercial sector and public administration discussed together with the BSI how an information society can be made both smart and secure at the same time.

Ideas on a secure information society were discussed during a think tank

Emphasising the exemplary role of government in the field of IT security, establishing legally binding standards for all IT products according to the principles of security and privacy-by-design and by-default, stimulating an intensive debate on the subject of liability in the field of IT security and creating an appropriate organisational framework: these are among the topics of the project "Digital Society: Smart & Secure." Its aim is to discuss the topic of cyber security in society with a broad spectrum of players to identify the need for action and to develop proposals for solutions.

WORKSHOP "SECURE INFORMATION SOCIETY"

The unofficial start-up of the project was the workshop "Secure Information Society" (BSI Magazine 02/2016), which was held by the BSI in April 2016. Seven theses for a secure information society were developed and passed by consensus agreement, but the issues discussed that didn't reach consensus, such as the security culture and the role of information security in digitisation, strengthened above all the BSI's intention to promote dialogue with different actors.

In the fall of 2016, a continuation of discussions was decided for the tried-and-tested format of the workshop with the "Digital Society: Smart & Secure" project and to accompany it with social research. A consortium from the nexus Institute and Digitale Gesellschaft e. V. together with ipsos GmbH and Dr. Ben Wagner as subcontractor will carry out the project on behalf of the BSI until February 2018.

JOINT DISCUSSIONS AND ANALYSES

In February 2017, 30 participants worked on issues of the aspects "security and technology," "trust" and "responsibility" in digital society. These findings flowed into various empirical surveys: a representative online survey was used to determine how the population is affected by various aspects of digitalisation and the importance of IT security. In addition, 20 citizens took part in an online community which made qualitative assessments.

Project team interviews with experts from civil society and science opened further perspectives on digital society and the role of different actors. The first results were presented to the participants in another workshop in June 2017. They too entered into the further discussions. By the end of the workshop, the jointly developed "Impulses on a smart and secure information society" had taken shape, supported by participants.

In the presence of BSI President Arne Schönbohm, participants in the process presented these impulses to the public on 7 September 2017 in Berlin. The subsequent panel discussion between representatives of the Federal Ministry of the Interior, the NRW Consumer Protection Agency, Amnesty International and Bitkom under the title "Security in the digital society" was particularly concerned with the question of marking of safe products and liability. Everyone involved in the project agreed on one point: the dialogue initiated with the project "Digital Society: Smart & Secure" and the dialogue started with the event series "Secure Information Society" should be continued and deepened. The impulse study is meant to act as a basis for this. ■

For more information see www.bsi.bund.de/susi

Three Seconds for More Email Security

Basic Tip from the BSI

Infected mail attachments or links to harmful websites contained in a mail are still among the most common ways to inject malicious software onto computers: If the recipients open their electronic mail too carelessly, the computer can be infected very quickly. The effects range from the infestation of individual computers to the failure of parts of the IT infrastructure and the loss of important data.

Is the sender known to you?
Invoice
Does the subject make sense?
Would you expect to receive an attachment from this sender?
Risks can be mitigated by performing a 3-second security check before opening an email.

PLEASE PAY CLOSE ATTENTION TO THE FOLLOWING POINTS WITH E-MAILS:

- The subject and text of the mail should be coherent and plausible
- Spam mails increasingly contain a correct address and other personal data
- Mails from well-known companies are often designed to be deceptively genuine
- Vague wording such as the subject “invoice” or “reminder” are an indication of spam mails
- Do not follow the request to open links or files
- Personal information shouldn’t be entered on websites that are linked to mails

For more information see
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/E-Mail/E-Mail_node.html

We Want Your Digital Perspective

Photos © iStock.com/Grafissimo; © iStock.com/Krasyuk

Federal Office
for Information Security

Information technology forms the foundation of modern life, making it all the more important for people to be able to trust the digital world; this is what we take care of. We are the national authority for cyber security, shaping IT security in Germany as well as in Europe and worldwide, working together with the worlds of commerce and science. We advise political and administrative bodies and are in dialogue with the public as well as a multitude of associations. Our experts are valued and sought-after in international discussion, and we do all this with one shared goal: information security. We ensure that the future will be able to grow from the network. With around 720 employees, we are a comparatively small team, but with huge responsibility – and that's why we need you with us.

For more information see www.bsi.bund.de/karriere and bewerbung@bsi.bund.de or phone +49 (0)228 99 9582 0

LEGAL NOTICE

Published by: Federal Office for Information Security (BSI)
53175 Bonn, Germany

Source: Federal Office for Information Security (BSI)
Section B23 – Cyber Security for Citizens; Public Relations
Godesberger Allee 185–189
53175 Bonn, Germany
Telephone: +49 (0) 22899 9582-0
email: bsi-magazin@bsi.bund.de
Internet: www.bsi.bund.de

Last updated: September 2017

Content and editing: Stephan Kohzer and Nora Basting, Federal Office for Information Security (BSI)
Joachim Gutmann, GLC Glücksburg Consulting AG,
Fink & Fuchs AG

Concept, editing and design: Fink & Fuchs AG
Berliner Straße 164
65205 Wiesbaden
Internet: www.finkfuchs.de

Printed by: Druck- und Verlagshaus Zarbock GmbH & Co KG
Sontraer Str. 6
60386 Frankfurt a.M.
Internet: www.zarbock.de

Item number: BSI-Mag 17/706e

Image credits: Title: Smileus/fotolia (top left), Gorodenkoff/fotolia (top right), Kasto/fotolia (middle left), BSI (middle middle), william87/fotolia (below left), Pressmaster/fotolia (below middle), Kiri/fotolia (below right), zapp2photo/fotolia (background); p. 2: Stephan Kohzer/BSI; p. 4: Henning Schacht (top left), Henning Schacht (below left), ECSM (below right); p. 5: NürnbergMesse it-sa (top left), NürnbergMesse (top middle), NürnbergMesse (top right), Geza Aschoff (below left); p. 6: R. Winkler; p. 8: BSI; p. 9: Bundesregierung/Güngör (top); BSI (middle left); BSI (middle right), BSI (below left), BSI (below right); p. 10: Wikipedia/BSI; p. 12: Bundespolizei; p. 13: Bundespolizeidirektion Flughafen Frankfurt/Main (top left), Bundespolizeidirektion Flughafen Frankfurt/Main (top right); p. 14: Fink & Fuchs AG (top left); p. 15: Fink & Fuchs AG (all pictures); p. 17: BSI (top left), BSI (top right); p.18: R. Winkler (top), BSI (below); p. 19: R. Winkler; p. 20 BSI; p. 21: BSI; p. 22: BSI; p. 24: BSI; p. 25: 1st row from left to right: Antonioguillem/fotolia, Bernardbodo/fotolia, Sepy/fotolia, miklyxa/fotolia, 2nd row from left to right: industrieblick/fotolia, Kadmy/fotolia, Georgerudy/fotolia, Antonioguillem/fotolia; p. 26: Joachim Gutmann; p. 28: Fink & Fuchs AG; p. 29: BSI; p. 31: Henning Schacht; p. 32 – 33: Fink & Fuchs AG; p. 35: BSI (all pictures); p. 36: BSI; p. 38: Foto Klein; p. 39: Foto Klein (top), Foto Klein (m.); p. 40: Peshkova/fotolia (background), Geza Aschoff (screen); p. 43: BSI; p. 44: BillionPhotos.com/fotolia; p. 45: BSI; p. 47: PwC Deutschland (all pictures); p. 48: travelview/fotolia; p. 49: Bayerisches Landeskriminalamt; p. 50: BSI; p. 51: BLKA; p. 52: Iconimage/fotolia; p. 54: BSI; p. 55: Pickup/fotolia; p. 56: genua gmbh; p. 58: BSI; p. 59: BSI; p. 60: Fink & Fuchs AG, Foto Can Yesil/fotolia; p. 61: Fink & Fuchs AG, Fotos: iStock.com/Grafissimo, iStock.com/Krasyuk

The BSI Magazine is published bi-annually. It is part of the Federal Office for Information Security's public relations work. It is provided free of charge and is not intended for sale.

Scan the QR code for the digital version of the BSI magazine
https://www.bsi.bund.de/BSI-Magazin

www.bsi.bund.de