Federal Office
for Information Security

BSI Magazine 2016/02

Security in focus

Europe and International Cooperation

BSI INTERNATIONAL

ANSSI: Portrait of a collaboration

BSI INTERNATIONAL

The eIDAS Regulation: Uniform framework conditions throughout Europe

THE BSI

25 years of the BSI

EDITORIAL

"Digitalisation and cyber security are two sides of the same coin."

Dear readers,

In 1990, the Internet was released for commercial use – a milestone in the history of IT. Since then, the World Wide Web has become a mass phenomenon that has become an integral part of our personal and working life. This has both positive and negative sides.

As commercial Internet use has increased, cyber crime has become a phenomenon which creates a greater sense of anxiety today than ever before.

In Germany, an early, pioneering response to the potential risks posed by the new information technology came in 1991, with the founding of the Federal Office for Information Security (BSI). Over the 25 years since then, it has become Germany's cyber security authority as the central point of contact for all aspects of IT security. To mark this anniversary, this issue of the BSI magazine includes statements of individuals who have helped shape and support the development of this authority.

This year, we are also celebrating another anniversary which reflects the rapid rise of cyber crime. Five years ago, the National Cyber Response Centre, was founded. This central cooperation platform pools the resources of the security authorities in Germany. Soon, it will also include all supervisory bodies via the operators of the critical infrastructures. After all, the people who commit cyber attacks aren't interested in administrative structures or official areas of responsibility. That's why when it comes to averting risk, cooperation is key.

This principle also applies beyond national borders. For this reason, France and Germany have been collaborating on cyber security systems for many years now. This close cooperation with the French agency for the security and protection of information systems, or ANSSI, is based on trust and shared attitudes to strategic issues, a common position with regard to defensive orientation and a similar high degree of technical know-how.

Certainly, the omnipresence of cyber threats may deter some companies from participating in the digital transformation and be a cause of anxiety to some Internet users. But at BSI, it is also part of our job to take these fears seriously and explain how we can protect ourselves. After all, digitalisation and cyber security are two sides of the same coin. That's why the BSI, as the national cyber security authority, is creating information security for the digitalisation process through prevention, detection and reaction on behalf of the state, business and society. We support you in learning how to use information technologies safely.

I hope you will find the articles informative and stimulating.

Bonn, September 2016

Arne Schönbohm,
President of the Federal Office for Information Security

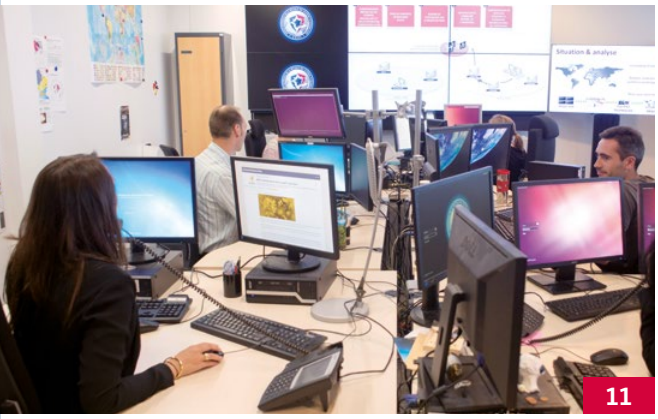


TABLE OF CONTENTS

IN BRIEF

BSI and VW

Working together for greater cyber security

The BSI and the group security division at Volkswagen AG have agreed to collaborate in the area of cyber security. The core element of the collaboration is the intensification of the exchange of information on cyber hazards. This information then flows into the BSI's overview of the current situation. In so doing, it contributes to a representation of the current hazards in the German cyber space and forms the basis for recommended measures to be taken. The goal is to work together to improve the overview of the current situation with regard to cyber security in order to be able to act more effectively to combat cyber crime. Volkswagen AG also joined the Alliance for Cyber Security.

ECSM

European Cyber Security Month

In October 2016, the BSI is again supporting and coordinating the European Cyber Security Month (ECSM) in Germany. Under the heading "Onto the Internet – safely", the BSI will provide information on the everyday hazards of the cyber world. Independent campaigns and joint activities with partners are designed to raise awareness among citizens and companies for a responsible and secure use of the Internet.

Since 2012, the member states of the European Union have been offering events, information and campaigns on the ECSM under the leadership of the European Union Agency for Network and Information Security, or ENISA.

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

Ranking

The BSI is again among the top employers

When the best employers in the IT sector in Germany were selected, the BSI reached 15th place, making it again one of the top employers in the field. Since 1999, the trendence research institute has conducted a survey of 5,700 IT students at 69 higher education institutions in Germany, asking them about their ideal employers and career plans, recording the results in the trendence Graduate Barometer.

Currently, the BSI is offering various application opportunities for specialists from the field of IT and mathematics, as well as engineering and the natural sciences. For information on current job offers at the BSI, visit https://www.bsi.bund.de/jobs.

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

ViS!T in Berne

Flying visit to Switzerland

This year, the BSI took part in the 8th ViS!T symposium in Berne. Employees of public administration bodies from Austria, Switzerland, Luxembourg and Germany met under the banner of "The specific application of IT security" to hold multilateral discussions on topics related to IT security. The common goal of the participating countries is to achieve a comparable and, if possible, binding IT security level.

The symposium, entitled "Administration integrates secure information technology", takes place every two years in the participating countries in rotation.

Ransomware

The level of threat remains high

On behalf of the Alliance for Cyber Security, the BSI conducted a survey on the degree to which German industry is affected by ransomware. The results clearly show how vulnerable many companies in Germany are to cyber attacks. According to the survey, a third (32 percent) of companies of all sizes questioned had been affected by ransomware over the last six months. In some cases, the impact was considerable: For one in five of the companies affected (22 percent), there was a significant failure of parts of the IT infrastructure, while 11 percent of those affected suffered a loss of important data.

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/ransomware-umfrage-2016-04.html

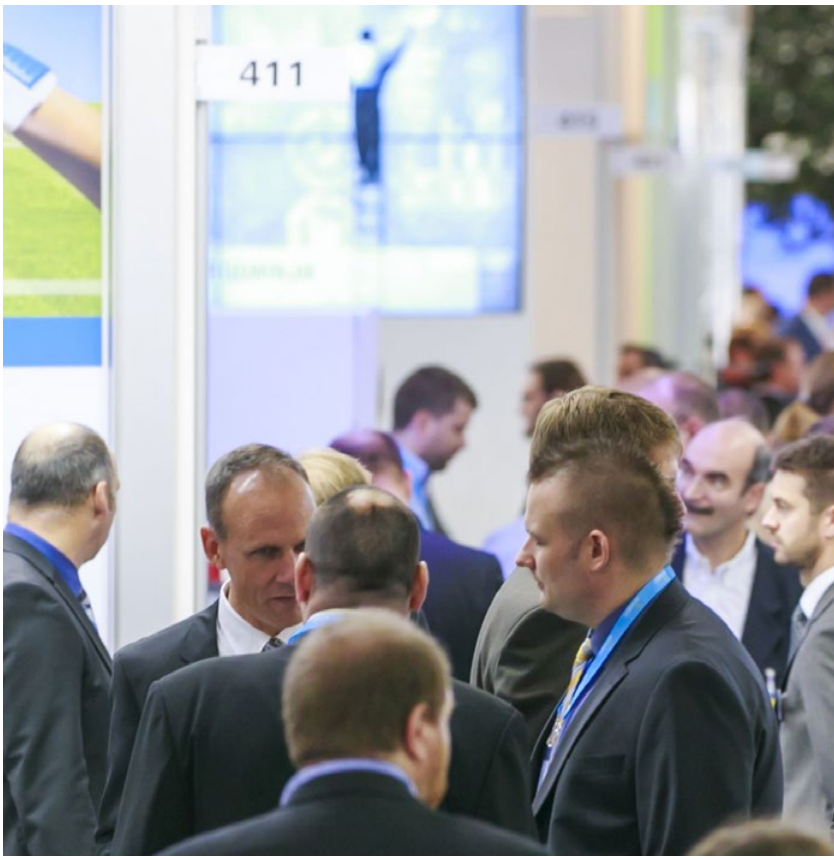
CSCG

Cyber Security Challenge Germany

One of the tasks of the Cyber Security Challenge Germany, which is supported by the BSI, is to find the IT specialists of tomorrow and support their development at an early stage. The competition is aimed at school pupils and students aged between 14 and 30, and is part of a Europe-wide initiative. New recruits and young people with experience are equally welcome to participate. At the end of September, the new young talents demonstrated their skills in the national final in Berlin. The winners were invited to take part in the European final, the European Cyber Security Challenge (ECSC) in Dusseldorf in November.

https://www.cscg.de

it sa 2016



by Thomas Philipp Haas, NürnbergMesse

The international showcase for the IT security sector

From 18 to 20 October 2016, the focus at the Nuremberg trade fair centre will again be on IT security. Around 480 exhibitors are expected at the eighth it-sa trade fair – more than ever before. They include not only companies and organisations from Germany, Austria and Switzerland, but also from Malta, Israel and South Korea. The growth curve is climbing steeply. In the last three years alone, around 100 new exhibitors have signed up for the fair. One important supplementary event to the it-sa is the Congress@it-sa conference programme. The BSI has provided ideas in support of the it-sa right from the start, and will this year again organise the IT-Grundschutz day on the second day of the fair.

"The it-sa covers all facets of cyber security", says Frank Venjakob, Executive Director of it-sa. At the it-sa, IT security experts gather information about products and services and discuss current IT security issues at the Congress@it-sa. In terms of its subject area, the event covers the entire range of IT security technologies available, from authentication through to wcertification, and provides a platform for consulting and training companies. Special areas for start-ups, on IT security when planning, constructing and operating data centres and on identity and access management round off the products and services exhibited. This makes the it-sa not only the leading event of its kind in Europe, but it has also become one of the most important IT security events in the world, attracting over 9,000 visitors.

JOINT STANDS FROM ISRAEL AND FRANCE

Once again, this year's trade fair demonstrates its international significance. For the first time, Israel and France will participate with joint stands. Neighbouring France is the third most important market for German foreign trade in terms of import volume. Start-up nation Israel is represented by a total of 17 companies at the it-sa.

GREEN, RED AND BLUE: EXTENSIVE FORUM PROGRAMME ON ALL SECURITY-RELATED ISSUES

Since the first event in 2009 the colours green, red and blue have represented the open forums in the it-sa supporting programme. In over 230 sessions and topic blocks, companies, associations and organisations can gather information on three presentation stages located right in the middle of the trade fair activity. Here, the focus is on current developments in IT security. The BSI will also be represented on 19 October with a speaker on the subject of cyber security in economy. The presentations in the blue forum focus on practice-oriented solutions and technologies for a secure IT and data infrastructure. CEOs, CIOs and individuals responsible for IT will find answers to strategic and business-related questions in the red forum. One of the highlights of the forum programme is the panel discussion on current developments with regard to FIDO (Fast IDentity Online), authentication standards and a focus on the EU basic regulation on data protection.

IT-GRUNDSCHUTZ DAY ENTERS THE NEXT ROUND AT THE IT-SA

Away from the bustle of the trade fair itself, the accompanying conference programme provides a framework for intensive expert discussions. The 4th IT-Grundschutz day will again take place in Nuremberg within the framework of the Congress@it-sa. On 19 October, the modules of the 15th updated version of the IT-Grundschutz catalogue will be presented, among other things. Another item on the agenda is the modernisation of IT-Grundschutz. ■

THE BSI AT THE IT-SA

From 18 to 20 October 2016 in the Nuremberg trade fair centre

For more information on all the exhibitors, their products, the hall plan and on all conference and forum presentations, go to: https://www.it-sa.de

BSI INTERNATIONAL

eIDAS

by Jens Bender, head of section eID-Technologies and Smartcards

In order to create a real European internal market in the digital space, the EU has created uniform framework conditions with the eIDAS regulation. Electronic business transactions and communication processes between citizens, companies and authorities can now also be conducted across national borders in a trustworthy, legally binding and above all secure way.

More trust in the digital internal market

Since 1 July 2016, consumers throughout Europe can sign electronic contracts on the Internet more easily. With the new EU regulation on electronic identification and trust services (eIDAS regulation), cross-border digital transactions will be simplified. Electronic signatures, seals and timestamps, as well as the delivery of electronic registered mail and the mutual recognition of electronic identification means, are now uniformly regulated for the entire European Economic Area (EEA). In addition, a new category of qualified website certificates has also been created.

While the eIDAS regulation does not repeal the German Digital Signature Act, it does take priority. In order to create greater clarity, the Federal Ministry for Economic Affairs and Energy (BMWi) is planning a Trust Services Act (VDG) which will replace the current Digital Signature Act.

MORE TRUST SERVICES

Trust services are those various services which are designed to ensure trust among citizens and businesses in the technical and legal security of cross-border digital processes. They include qualified electronic signatures and timestamps. A new addition are qualified electronic seals for companies and public authorities, the qualified delivery of electronic registered mail (such as De-Mail) and qualified certificates for website authentication. The eIDAS regulation on these trust services aims to make it possible to trade on the electronic internal market in a legally secure way and with the same level of trust as with traditional, paper-based procedures. The prerequisites for this are suitable security and interoperability standards, checking for compliance with requirements by means of audits, certification and monitoring of providers and the stipulation of the legal effect of the various services.

The BSI has described the classification of trust services and the various methods of electronic identification into a range of different trust levels in TR-03107-1, "Electronic identities and trust services in e-government – trust levels and mechanisms".

While the legal effect of the services is stipulated in the regulation itself, the standards are left to the standardisation bodies such as CEN, ETSI and ISO. For many areas, the BSI is providing its own technical guidelines (such as the TR-03145, "Secure CA Operation") and is an active participant in the standardisation process.

The trust services providers will be monitored by national bodies. The BMWi has nominated the Federal Network Agency to the EU Commission as the authority responsible for signatures, seals, timestamps and delivery services, and the BSI as the agency responsible for website certificates. Users can recognise the qualified trust services on provider websites through the standardised EU trust seal.

REMOTE SIGNATURES AND WEBSITE CERTIFICATES

Until now, a signature card has been required in all cases for a qualified electronic signature in Germany. eIDAS now makes it possible to also create what is known as a remote signature (or server signature). These enable the user to store their personal signature key with a trust services provider and have the provider use it to sign their documents. This is particularly beneficial to users who only seldom need signatures.

In order to meet the security standards (such as ensuring the authenticity of the user), the European Committee for Standardization (CEN), with support from the BSI, has developed the corresponding guidelines and protection profiles for trust services providers. As one component of this, a secure, 2-factor authentication is required. In Germany, the eID function of a user's ID card is suitable for this purpose.

Additionally, the qualified website certificates category will also be introduced for SSL/TLS website certificates in order to achieve greater trust in them.

ID CARDS CAN CROSS BORDERS

The eIDAS regulation also aims to achieve simple, cross-border use when it comes to electronic identification.

For a long time now, ID cards have made it possible to travel across borders within Europe. However, the online identification function also provides a secure base for the use of electronic services.

At the same time, national eID systems are already in place in other EU member states. For this reason, they will not be replaced by a uniform system; instead, the eIDAS regulation aims to create interoperability between the national systems.

The eIDAS regulation regulates the framework conditions required for mutual recognition. The member states can notify their national eID systems to the Commission. While notification is offered on a voluntary basis, the recognition of notified eIDs (for the public sector) will be mandatory from 29 September 2018 onwards.

Here, the choice of means of identification depends on the level of trust required for a service in each case. The higher the trust level, the more secure the eID system needs to be.

The cross-border interoperability will be implemented by the Interoperability Framework specified by the member states, with Germany represented by the BSI. It can be securely and flexibly integrated into the respective systems of the member states and transferred between them.

German authorities must now create the preconditions to enable citizens and companies from all EEA states to use their national (notified) eIDs with German administration services.

On the other hand, holders of an electronic residence permit or ID card will in the future also be able to simply and securely identify themselves electronically to public authorities and service providers in other EEA states using the eID function. Here, the eID function of the ID card meets all the requirements for notification at the highest level of trust.

The BSI, together with partners from the industrial sector, has conducted the preliminary technical work required for the integration of ID cards into the systems of other member states. The first test projects with other EU countries are already running. ■

https://www.bsi.bund.de/eidas-vo

https://www.personalausweisportal.de/DE/Verwaltung/eIDAS_Verordnung_EU/eIDAS_Verordnung_EU_node.html

WORKING TOGETHER FOR A SECURE DIGITAL EUROPE

by Dr. Guillaume Poupard, Director General of the French cyber security agency ANSSI

France and Germany cooperate for cyber defence

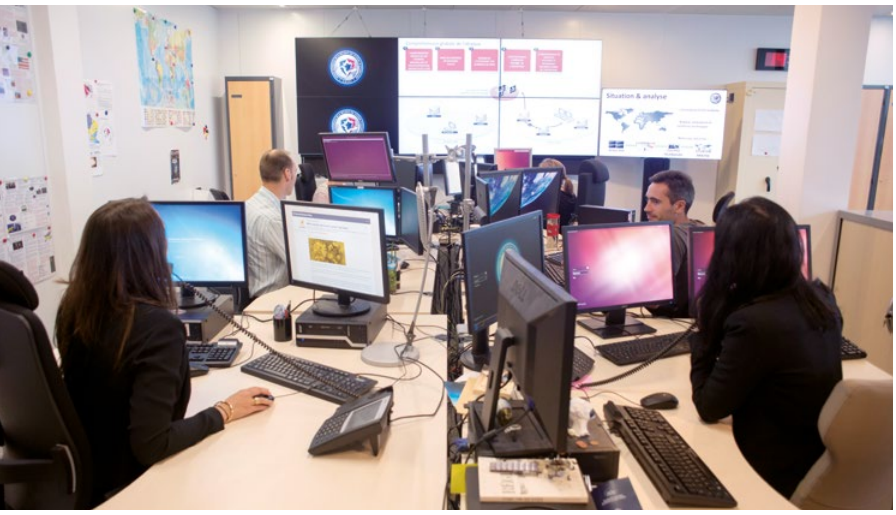
Facing a growing number of sophisticated cyberattacks over the years, France decided a decade ago to reinforce its technical and operational capabilities to respond to these threats on both national and international levels.

With the publication of the 2008 White Paper on Defense and National Security, France formally acknowledged that information and communication systems had become essential to the proper functioning of its society, whose growing reliance on ICT had made prevention and reaction to cyberattacks two major priorities in the organization and planning of national security.

As a response to this strategic shift, the Agence nationale de la sécurité des systèmes d'information (ANSSI) was created in 2009 and became the national authority for cybersecurity and cyberdefence with the mission to foster a coordinated, ambitious and pro-active response to cybersecurity issues in France.

In 2013, years of experience and cooperation with critical operators led the French government to propose the adoption of a regulatory critical information infrastructure protection framework to establish a common minimum level of cybersecurity for all critical sectors. This law now applies to more than 200 public and private operators who must follow security requirements to protect their most critical information systems and rely on approved service providers for audits, detection, incident response and remediation.

While cybersecurity of administrations and operators of vital importance remains a high priority for France, recent years have also shown that cybersecurity no longer concerns only governments and large businesses but also businesses of all sizes in every sector of the economy as well as private citizens themselves. Today, our mission is also to contribute to the protection of citizens' digital lives, privacy and personal data. Therefore, France will soon launch a new platform to assist the victims or cybermalevolent acts. This public-private partnership will fulfill different missions from helping citizens, Small and Medium-sized Enterprises (SMEs) and local administrations to identify their security problems, to providing a list of service providers and raising awareness among the general public.



Profile in brief:

Dr. Guillaume Poupard has been Director General of the French cyber security agency ANSSI (Agence nationale de la sécurité des systèmes d'information) since March 2014. Previously, the doctor of cryptography worked in the French Ministry of Defence and in the DGA procurement authority in the field of cyber security.

To fulfil its missions, the Agency and its 500 experts currently deploy a broad range of regulatory and operational activities, from issuing regulations and verifying their approval, to the certification and accreditation of products and service providers, the monitoring of networks and the incident response in case of a major attack.

COOPERATION IN CYBERSPACE IS ESSENTIAL

In a world that is increasingly interconnected, it does not make much sense for a State to tackle digital security issues on its own. Unveiled by the French Prime Minister in October 2015, the new French digital security strategy states France's will to engage a dialogue both within multilateral organizations and with long-term trustworthy partners following two objectives: contributing to the global stability of cyberspace as well as reinforcing the States' own cybersecurity.

Germany is one of the strongest and most natural allies for France in many areas of cooperation, including cyber-security. The longstanding and close bilateral cooperation between ANSSI and BSI is based on trust and has been greatly facilitated by a shared vision on many strategic and political issues, a common positioning at the national level fulfilling only defensive missions and a comparable high level of technical expertise. Moreover, the 25 years of experience that BSI is now celebrating reflects the already long-lasting history that we share in the field of cyber-security.

While the scope of actors preoccupied by their digital security has widen, so has our daily work which is no longer restricted to the development of technical and operational capacities but is also about defining efficient governance models, adopting adequate regulations, establishing dialogue with relevant public and private stakeholders, or engaging with other countries and multilateral organizations, starting with the European Union (EU); in other words, using all available levers to safeguard the digital security of the Nation as a whole.

On that matter, the recent adoption of the EU Directive on Network and Information Systems Security (NIS) will allow a common minimum level of cybersecurity preparedness and response in Europe, thus ensuring the smooth functioning of the EU Single Market.

With the support of French President François Hollande and the German Chancellor Angela Merkel, ANSSI and BSI have been working together in many fields, such as cloud-computing with the creation of a common label for secure cloud service providers, security certification though a very strong support of the international recognition schemes (CCRA and SOG-IS) and industrial synergies via a dedicated meeting during the last International Cyber-security Forum (FIC) in Lille. To build up on these successes, our cooperation scope will be widened and developed in the future in order to raise the level of cybersecurity in France, Germany and more largely within the European Union.

TOWARDS THE EUROPEAN STRATEGIC AUTONOMY IN THE DIGITAL DOMAIN

Even if States are primarily responsible for their national digital security, it is France and Germany's shared vision that many challenges can best be addressed through a common and coordinated effort at European level.

Beyond the development of EU Member States' capacities and cooperation, the EU must as well recognize that European digital security is challenged on other fronts, requiring a collective ambition to guarantee Europe's digital sovereignty. Three challenges in particular are ahead of us:

1. the EU and the Member States' ability to protect and defend the EU institutions, the administrations, the critical infrastructures, the companies and the general public in cyberspace must be ensured;

2. the EU must actively support the development of sustainable European industries in the field of digital security and guarantee Member States' ability to evaluate and approve the security of digital products and services;

3. the EU must preserve its capacity to choose autonomously how data and related services should be protected in Europe.

Along with like-minded Member States, France and Germany will closely work together to promote the European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of our values.

JOINT CONCLUSION OF THE LAST FRENCH-GERMAN DEFENSE AND SECURITY COUNCIL (07/04/2016):

Germany and France are jointly pursuing the goal of achieving strategic independence for the EU in the digital age by means of the following steps:

1. Strengthening the ability of member states and the EU as a whole to protect their networks and increase their digital resilience through the joint call to quickly implement the NIS [Network and Information Security] guideline;

2. The development of an independent, innovative, effective and diversified European industry, in particular with regard to the generation of trust in the digital environment and cyber security;

3. A guarantee of the ability of Europeans to decide on the safety level of their data independently, in particular in connection with trade deal negotiations.

Germany and France have taken several initiatives in this area, such as by making joint efforts regarding the certification of security of Cloud computing or the security of e-mails, the organisation of "speed dating" between German and French SMEs working in the field of cyber security on the fringe of the International Forum for Cyber Security in Lille in January 2016, or through their combined work to promote international cyber security at a diplomatic level, in particular in the United Nations, the OSCE, the EU and NATO.

ANSSI IN FIGURES

500 experts today – **100** recruitments planned in 2016.

Nearly **30** major French IT attacks dealt with in 2015.

More than **20** technischen Publikationen in 2015.

More than **150** instruction operations carried out in 2015 to raise awareness.

1,500 State agents trained annually by ANSSI on information-system security problems.

Further information:
http://www.ssi.gouv.fr/en/

The creation of the ANSSI-BSI Cloud Label

by Dr. Clemens Doubrava, section Information Security in the Cloud and in Applications

How a new European initiative is being created based on trust and expertise

ANSSI (Agence national de la sécurité des systèmes d'information) and the BSI have been very intensively involved with the security of Cloud Computing in recent years. Both authorities arrived at a very similar understanding of the Cloud security standards that need to be met, and both initiated new ways of verifying secure Cloud Computing, since the existing certifications failed to adequately meet the needs in this area. However, both authorities pursued different paths.

AUDITING BY PUBLIC AUDITORS

The BSI developed the Cloud Computing Compliance Controls Catalogue (C5). This catalogue, which is closely oriented to tried and tested standards, defines the requirements for the secure provision of services critical to businesses, which the Cloud provider must meet. Additionally, the provider must make their offer transparent, such as the location of data processing and the subcontractor. The auditing process is conducted in line with the international recognised standard, the ISAE 3000. The audit report is based on standards such as the ISAE 3402 and SOC 2. Auditors and Cloud experts conduct this audit and issue an audit opinion, for which the auditor bears liability. The C5 also contains standards for greater protection needs and can be individually extended – for example for a specific industrial sector. The BSI sets the standards and specifies criteria for the audit, but has no further supervisory role with regard to specific procedures.

THE ANSSI PERFORMS ITS OWN CERTIFICATIONS

The ANSSI takes a very different approach. The Référentiel SecNumCloud, which is strongly oriented to the ISO/IEC 27001 standard and which supplements it with several specifications of its own, defines the standards required for secure Cloud Computing. In the Référentiel, there are two levels: sécure and sécure plus, whereby the latter sets higher security standards and limits to France the service provided. Taking this as a basis, the ANSSI has developed a completely new certification of its own, which it has established in France. Cloud providers receive a certificate which is issued by the ANSSI and on which an audit report produced by ANSSI-certified auditors is based.

A SHARED CLOUD LABEL IS BEING CREATED

While the security levels which the BSI and ANSSI would like to see in place are very similar, the two very different approaches towards certification and attestation appear to contradict each other.

Motivated by the German-French business consultations and based on a high level of mutual trust, the idea therefore emerged of generating a new Cloud Label. It stands for the joint Cloud security standards and is suitable evidence that they have been met. The underlying principle on which the label is based is a joint short catalogue with security targets (“core rules”). Naturally, the attestation in accordance with the BSI’s C5 and the ANSSI certification are sufficient to meet these standards. A provider who already has one of the two certifications can receive this label and as such advertise the security level of their product very easily on both markets.

The Cloud Label is regarded by the ANSSI and BSI as being an explicitly European initiative, which can also incorporate the certifications of other countries. In this way, the expertise and independent nature of the BSI and ANSSI, as well as their cooperation based on trust, are of benefit to the whole of Europe. ■

Further information:
https://www.bsi.bund.de/cloud

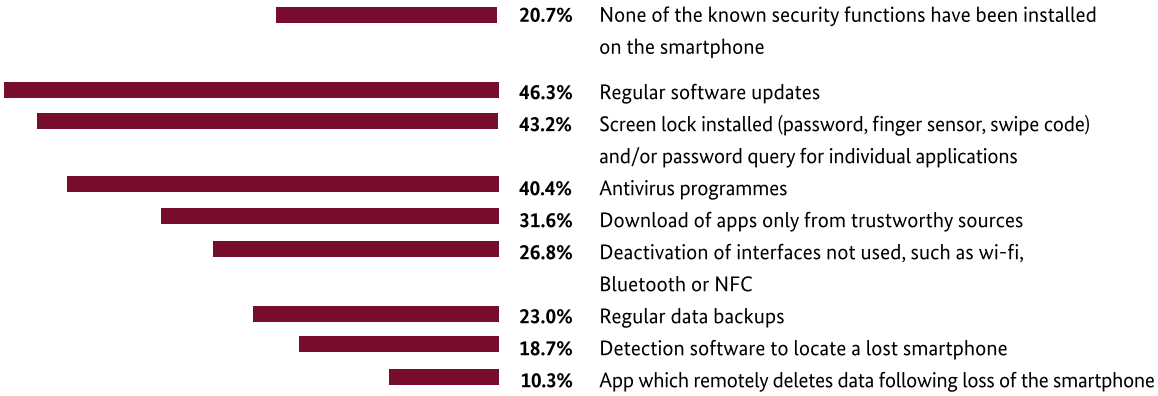
CYBER SECURITY

The transparent smartphone user

Majority of Germans are exposed to security risks

ONE IN FIVE SMARTPHONE USERS ARE WITHOUT SECURITY PROTECTION

What security functions do you use on your smartphone?



THE YOUNGER GENERATION IS MORE CAUTIOUS IN THE WAY THEY USE SMARTPHONES

92.5%

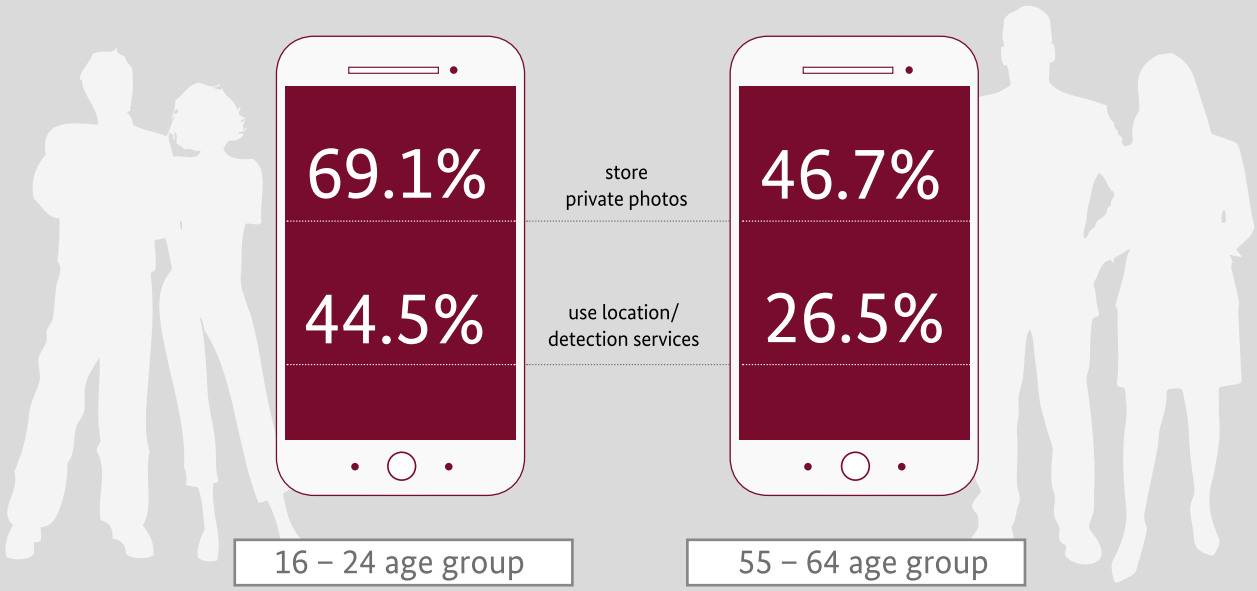
of 16 to 24-year-olds confirm that they use one or more of the above security functions

66.8%

of 55 to 64-year-olds confirm that they use one or more of the above security functions

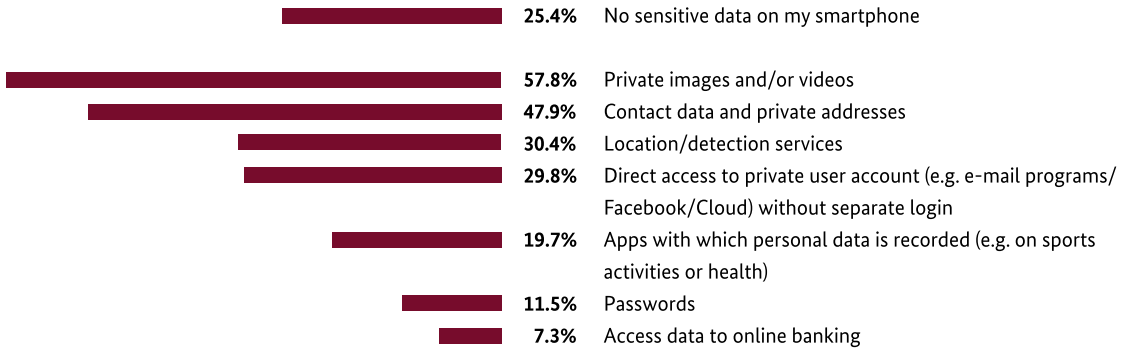
Source: Representative online survey conducted on behalf of the BSI by TNS Infratest GmbH.

THE YOUNGER THE SMARTPHONE USER, THE MORE SENSITIVE THE DATA STORED ON THE SMARTPHONE



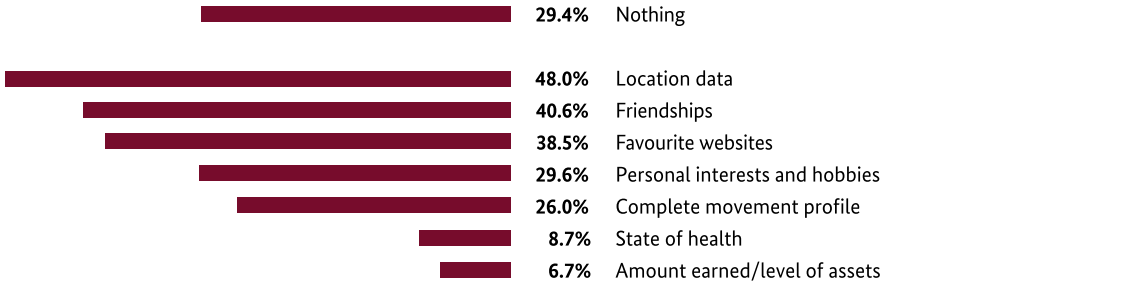
SENSITIVE DATA

What data do you store on your smartphone?



VOLUNTARY SURVEILLANCE BY THE SMARTPHONE

What do you think your smartphone knows about you?



Further information: https://www.bsi-fuer-buerger.de/smartphones

“The German certification scheme enjoys an excellent reputation worldwide”

Interview with Dr. Markus Mackenbrock

It is not just the BSI whose 25th anniversary is being celebrated in 2016. It has also been issuing certifications for a quarter of a century. Over 1,000 certification processes have been completed from the time the first certificate was issued to the present day. Dr. Markus Mackenbrock, head of the BSI’s section Recognition of Expert Bodies and Quality Management, offered us an insight into this special field of the BSI’s work.

The BSI acts as the central certification office for IT security in Germany. That sounds like a lot of work. How is the BSI organised in this respect?

Fortunately, the BSI is not solely responsible for the test procedure. Instead, the products are currently tested by nine test centres throughout Germany in accordance with the defined certification schemes. These test centres have undergone a recognition procedure in conformity with the stipulations specified by the BSI, and perform these tasks on behalf of the BSI specifically in the field of common criteria (CC). Common criteria is a recognised international standard for testing and assessing the security features of IT products. Our certificates have an excellent reputation worldwide, and many foreign product manufacturers apply for CC certification from us – also because we work particularly efficiently and with a focus on client needs.

There are other standards in place aside from common criteria. How do you differentiate between them, and where are the areas of application?

Common criteria relates solely to the security features of products for which functionality and interoperability are the

Profile in brief:

Dr. Markus Mackenbrock has been working at the Federal Office for Information Security (BSI) since 1993, and played a key role in helping to shape the first 10 years of the development of the common criteria (CC). Today, he is responsible for the recognition of CC test centres and for training CC assessors.

focus of the technical guidelines. The ISO/IEC 27001 international standard describes an ISMS (Information Security Management System) for a self-contained network such as a data centre or IT division. We also certify auditors and IT security services. Here, there is a great deal of potential for development, since the market for IT security services is experiencing strong growth at a time of increasing cyber threats.

In 25 years, the IT world has witnessed a very large number of fundamental changes. I assume that this also applies to certifications?

What has changed more than anything else is the complexity of the products to be certified and as a result the necessary degree of thoroughness of the testing process. Today, we are often confronted with assembled products, the individual components of which need to be certified, such as the hardware, system software and application. The aim is then to produce a certificate for the entire assembled product. Initially, things were different, with the focus mainly on just the system software or application. The amount of time spent on the tests themselves has also increased, since today, greater thoroughness is needed. This is a result, among other things, of the greater variation in the possible ways of attacking a product. In spite of all this, we issue far more certificates today – around a hundred every year - than we did during the early years, when at most it was just a handful.

Have the types of product that you certify also changed?

Yes, in fact to a very large extent. During the early years, we did not yet certify hardware. This has changed in particular since the introduction of smartcards. And today, we also certify end user products such as smart meters or the electronic ID card. Before, from the consumer point of view, certificates were only given to exotic niche products.

Currently, the word on everyone's lips is digitalisation. What influence do these fundamental developments have on your work and on the significance of certification procedures?

We are currently developing a large number of new test regulations in the areas of energy management, health, the automotive industry and critical infrastructures. In this respect, we are involved in the development of the security standards, which already need to be taken into account during the development process of products. Here, the ISMS is of great importance, since in the health sector, for example, the entire infrastructure needs to be taken into account, from the electronic health card through to the reading device and the encrypted transfer of sensitive information. Also, there are an increasing number of specific legal requirements for a BSI certification, such as for ID cards and the health card, as well as smart meters and digital tachographs. These topics, which will be of relevance in the future, account for a large part of our work.

Further information: https://www.bsi.bund.de/EN/certification

NEW FOUNDATION FOR IT-GRUNDSCHUTZ

by Katrin Alberts, IT-Grundschutz section

Faster, safer, further: The BSI gets the tried and tested management system into shape for the new security requirements

Reason enough for even more protection: the IT-Grundschutz is the central management system for information security, which the BSI has been offering public administration bodies and businesses for 20 years. The BSI is currently making fundamental changes to the tried and tested method. The aim is to make the IT-Grundschutz even faster and more efficient to use in the future.

In principle, it can happen to any company: an online games provider becomes the victim of a hacker attack. The perpetrators gain access to confidential data of millions of users worldwide. For security reasons, the gaming website is taken off the Internet for several days, and the incident is investigated. For the company, the hacker attack results in damage to their image and financial losses.

Another scenario: a medium-sized company makes the unpleasant discovery at a trade fair that a very high-quality product that it has patented has been copied by an Asian company, which has produced a cheap, plagiarised version which has been copied and exhibited. Since the negative impacts on sales as a result of plagiarism could endanger the company's existence, the executive management orders an examination of information security. Various weak points are discovered and rectified in order to avert future attempts at spying.

A WIDE RANGE OF CHALLENGES FOR COMPANIES

Both scenarios have one thing in common: they reflect everyday reality when it comes to information security in Germany. There are many different reasons for incidents involving breaches of information security, with serious consequences in some cases: On the one hand, the innovation cycles in which further developments in information technology are made are becoming shorter. On the other, today's technical systems are becoming increasingly complex. At the same time, a growing number of areas of public life and business are exposed to an increasing level of dependence on well-functioning information technology. These circumstances lead to a situation in which for many companies and institutions, cyber security is no longer a purely technical matter related to IT operation, but is a management task. In the meantime, managers also have to deal with the issue of the potential effects of a cyber attack on the institution. Aside from this, customers, suppliers and business partners can also be affected. For this reason, a well-planned, organised approach among all those involved is needed in order to establish and maintain a suitable and adequate level of security.

As an established management system for information security, the IT-Grundschutz takes into account the more stringent, more dynamic requirements for securing information, with the tried and tested method currently being fundamentally revised. The aim is to help generate a significant increase in information security in the field of administration and business.

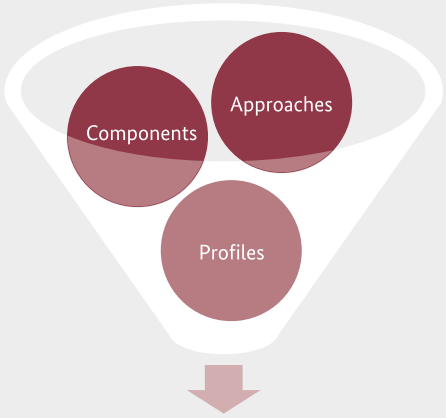
IN FOCUS: MEDIUM-SIZED BUSINESSES

Due to the incredibly rapid changes in the threat level for IT systems, the IT-Grundschutz is increasingly focusing on the issue of cyber security. For this reason, greater emphasis is placed there on detecting cyber attacks and reacting in an

appropriate way. At the same time, it should be possible to produce and publish all IT-Grundschutz publications, such as the tried and tested modules, in a faster and more flexible way in the future. This will ensure that the IT-Grundschutz will be in line with the latest technology developments at all times.

As well as public authorities and larger industrial companies, the aim in the future is to address small and medium-sized enterprises (SMEs) in a more concerted way. Due to a lack of personnel and financial resources, SMEs are usually more vulnerable when it comes to information security than larger institutions.

CORE ASPECTS OF MODERNISATION



NEW APPROACHES MAKE IT EASIER TO GET STARTED

In the future, institutions will be able to choose from three different approaches.

1. The basic protection provides fundamental security for an institution's business processes and resources. It enables the first steps to be taken in the security process in order to reduce the biggest risks as quickly as possible. As a next step, the actual security requirements can be analysed in detail. This approach is therefore particularly suitable for SMEs.

2. The core protection acts as a further initial process in order to protect the essential business processes and resources. This approach differs from the classic IT-Grundschutz by focusing on a small but very important element of an information network.

3. The standard protection preferred by the BSI corresponds in terms of its basic features to the known IT-Grundschutz approach according to the current BSI 100-2 standard. The new IT-Grundschutz concept is also designed to cover an even broader topical spectrum. Automation, process control and process management systems (Industrial Control Systems, ICS) as well as detection and reaction have also been included, for example.

GOAL: SECURITY STANDARDS FOR SECTORS

Another new development comes in the form of what is known as the IT-Grundschutz profiles. With these profiles, the BSI provides a flexible package with which user groups can adjust the IT-Grundschutz to meet their specific needs and then publish them for other interested users. In the next step, the IT-Grundschutz profiles provide the basis for developing and continuously updating sector-specific security standards. As well as passing on know-how, companies and authorities with the same security issues can network, and both sides can profit from the experiences of other institutions. It future, it will be possible for institutions of all sizes to use the new IT-Grundschutz packages to secure their information networks.

TEAMWORK: USERS ARE AN IMPORTANT PART OF THE ITERATIVE PROCESS

The first modules have already been published during the complex process of modernising the IT-Grundschutz method. In a new publication process, these will now be made available for comments by users of the IT-Grundschutz in the form of "community drafts" on the IT-Grundschutz website. With the input from practical experience, the content can be further optimised to become a finished module. The first community drafts, including those relating to server, client and personnel security, have already been published for comments. Around 70 further modules are planned by the end of 2016. The multi-layer modernisation is due to be completed in 2017. The modernised IT-Grundschutz will continue to support certification in accordance with ISO 27001. The BSI will inform the IT-Grundschutz community at an early stage as to which transition periods apply to certificates. The change from the old to the new IT-Grundschutz approach will be designed by the BSI in such a way that users can plan and design their individual change in a way that suits them best.

The IT-Grundschutz provided by the BSI makes a fundamental contribution towards increasing the level of information security in Germany. ■

Further information:
https://www.bsi.bund.de/EN/itgrundschutz

SUCCESSFUL TOGETHER

Five years of the National Cyber Response Centre

Cyber attackers aren't interested in administrative structures or clearly designated official areas of responsibility. That's why close cooperation and ongoing communication are important when averting risks. Only in this way can effective detection be turned into effective prevention.

In 2011, this insight led to the establishment of the National Cyber Response Centre. It is one of the core components of the cyber security strategy agreed by the German federal government in 2011 in order to optimise operative collaboration in cyber security and coordinate protection and security measures. This is based on an end-to-end approach, which draws together the different risks in cyberspace: cyber espionage, cyber surveillance, cyber terrorism and cyber crime. The goal is to promote faster information exchange, rapid assessments, and specific recommended measures derived from them.

CLOSE COOPERATION, CLEAR DIVISION OF AREAS OF RESPONSIBILITY

Cyberspace includes all information infrastructures that can be accessed via the Internet worldwide. In Germany, all areas of social and business life make use of the opportunities provided there. In a networked world, the state, critical infrastructures, the economy and the general population in Germany are dependent on the smooth functioning of information and communications technology and the Internet.

The Cyber Response Centre compiles all information known to the security authorities about cyber attacks on these information structures. Everyone shares and evaluates their new knowledge here, with every authority doing so from their perspective and within their area of responsibility.

In the central cooperation organisation of the German security authorities responsible for defence against electronic attacks on IT infrastructures, the BSI works alongside the Federal Office for the Protection of the Constitution (BfV), the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Office (BKA), the German Federal Police (BPol), the Central Customs Authority (ZKA), the German Intelligence Service (BND), and the German Armed Force (Bw). Soon, it will also include all supervisory bodies via the operators of the critical infrastructures. Each of these authorities seconds a member of their staff to liaise with the Response Centre. They all work together in a spirit of cooperation and have the same level of authority.

In the Cyber Response Centre, all authorities benefit from the shared knowledge in their respective areas of responsibility. In order to ensure that this functions smoothly, the Cyber Response Centre is networked with the Situation Centres and corresponding agencies of the participating authorities. While the BSI assesses a cyber attack from an information technology perspective, the BfV, the Military Counter-Intelligence Service (MAD) and the BND focus on the intelligence aspects. The areas of interest to the police are covered by the BKA, the ZKA and the BPOL. Finally, the BBK assesses the disaster prevention aspect and the needs of the critical infrastructures.

Understandably, close cooperation of this nature raises the question of whether the statutory duties and authorisations are also observed during the process. To ensure that this is the case, special administrative agreements are signed between the authorities involved. They have been shown to be extremely resilient over the last five years since the Response Centre was founded.

A COMPREHENSIVE OVERVIEW OF THE SITUATION, WELL-FOUNDED RECOMMENDED MEASURES

The Cyber Response Centre has moved forward in line with the changing level of risk since 2011. It has developed from a pure information hub into a central cooperation platform for IT security authorities.

This is due in particular to the developed routines and products, to a growing level of trust between the authorities involved, and to the staff who work at the Centre. They have developed a team spirit which spans all authorities involved, and collaborate in a targeted, highly integrated and efficient way within the framework of established processes, in the daily meetings to discuss the current situation, in working groups on specific topics and in joint visits to victims of cyber attacks.

NEEDS-BASED PRODUCTS, A WIDE RANGE OF SYNERGIES

The Cyber Response Centre products have also proven to be effective and robust. First, there is the cyber situation as an initial assessment which is updated on a daily basis. It presents cyber security issues in a needs-based, target group-oriented and structured way, with a high level of relevance in the field of technology, politics and the media. Additionally, there is

the information provided by the National Cyber Response Centre, which is used to produce an analysis used to reach a conclusion in an assessment of important issues on which the Cyber Response Centre panels focus their work.

A feature of both products is that all the participating authorities are involved, with their skills and within their scope of responsibility. Here, intelligence and police information is also given equal weight. It is precisely the political-ministerial target group addressed by these products which has a need for a consolidated view. It offers considerable added value over individual opinions.

The products are merely a measurable output of the wide range of synergies which result in particular from the regular transfer of knowledge in the Cyber Response Centre. While the participating authorities and institutions might continue to retain their individual responsibility for all operative tasks, depending on their official area of competence, a deep understanding of the requirements and unique features of each area of work has developed which extends far beyond the staff directly involved in the Cyber Response Centre. It not only provides sustainable cyber defence. It also makes it possible to pre-empt situations and know where attacks are likely to come from. In this way, useful and effective preventive action can be taken.

This is all the more important since one further aspect of the Cyber Response Centre's work is becoming increasingly significant, namely its coordination role. Today, the Cyber Response Centre coordinates the work on issues which affect the area of responsibility of several authorities through working groups which are specifically set up for each case ("coordinated case work"). Here, the Cyber Response Centre staff draw on appropriate additional resources from their respective institutions.

Nationales Cyber-Abwehrzentrum

The National Cyber Response Centre is based at the BSI in Bonn.

Over the past five years, the Cyber Response Centre has further developed both its organisational structure and the focal areas of its work and models of cooperation. It has shown itself to be flexible and efficient. And it has made a decisive contribution towards improving the cyber security architecture. ■

https://www.bsi.bund.de/cyber-az

The IT Security Act is mandatory – UP KRITIS is optional

by Nora Apel, section Critical Infrastructures – Principles

On 25 July 2015, the IT Security Act came into force, giving the BSI new responsibilities and powers in the area of Critical Infrastructures. The Critical Infrastructures provide important assets and services, some of which are vital, without which public and private life in Germany could no longer function in the way we have come to know it.

The IT Security Act demands that the operators of certain Critical Infrastructures report significant IT malfunctions to the BSI and to secure their IT which is necessary for the provision of critical services in line with the latest technological developments. The specific KRITIS operators who are subject to the new regulations are identified on the basis of a legal decree which is issued in two parts (or "sections") by the Federal Ministry of the Interior (BMI).

THE DECREE COMES INTO FORCE IN STAGES

The first section came into force on 3rd May 2016 and regulates the energy, water, food and information technology and telecommunications sectors. Systems operators covered by this decree must send a report to the BSI via a point of contact if an IT malfunction occurs. Through this point of contact, they also receive warning and situation products from the BSI.

Two years after the decree has come into effect at the latest, the operators must provide evidence to the BSI that adequate IT security measures have been taken which are of key importance to the ability of the Critical Infrastructures operated by them to function correctly. The second section of the decree regulates the transport and traffic, finance and insurance, and health sectors and is planned for the spring of 2017.

QUANTITATIVE AND QUALITATIVE CRITERIA

The KRITIS systems which are governed by the IT Security Act are identified using quantitative and qualitative criteria with the Method for Identifying Critical Infrastructures (MICI).

The qualitative criterion is the delivery of a critical service. This includes services of importance to the population, some of which are vital, the impairment of which would result in considerable supply shortages, impediments to public safety or comparable drastic consequences.

A level of supply was set for the quantitative criterion. Systems which – directly or indirectly – (can) supply 500,000 people or more are subject to the decree. For easier application, the level of supply was converted into values typical for the systems, such as the capacity of a system or the quantity produced per year.

Example: In Germany, the average amount of electricity consumed per person, per year is 7,375 kWh (including the converted consumption by companies). A power station which produces 420 MW or more net nominal output therefore supplies 500,000 people with a critical service (electricity supply), making it subject to the decree. Since failures or impairments among systems of this size are critical and can quickly lead to a supply crisis in Germany, such occurrences must be prevented.

UP KRITIS: COOPERATION BETWEEN BUSINESS AND THE STATE

As well as representatives of the BMI, the BSI and the BBK (the Federal Office of Civil Protection and Disaster Assistance), the regulators responsible and the specialist bodies at federal level, the operators of Critical Infrastructures were also involved in the drafting of the legal decree. The act is being implemented in cooperation within the UP KRITIS corporate partnership body. KRITIS operators, public authorities and associations have been working together to protect Critical Infrastructures since 2007. This cooperative approach taken by UP KRITIS to protect Critical Infrastructures will continue with the IT Security Act. ■

https://www.bsi.bund.de/IT-Sicherheitsgesetz

THE BSI

Greeting by Dr. Wolfgang Schäuble, Federal Minister of Finance

Dear readers,

In 1991, when I took responsibility as Federal Minister of the Interior for the founding of the Federal Office for Information Security (BSI), no-one could have known just how quickly digitalisation would spread. Even today, we cannot be entirely sure what the consequences of this change will be. Innovative business models are being created. New opportunities are arising for political and social participation. At the same time, criminal and terrorist networks are abusing the digital infrastructure.

For 25 years now, the BSI has been responding to the constantly changing threats posed by cyber crime – and with success. This is certainly due in part to the fact that, in addition to the technological opportunities for detecting and averting cyber attacks, the legal framework has been constantly adapted. As a result, since the BSI Act was amended in 2009, the BSI has been responsible for IT security among all federal public authorities. The IT Security Act of 2015 further increased the information security of critical infrastructures. Both acts are of key importance in the fight against cyber crime.

In Europe and at international level, the German federal government is promoting a strengthening of cross-border IT security. Due to the high degree to which our application systems are networked worldwide, cyber attacks in other countries are having an increasingly severe effect on IT security in Germany. It is precisely here that the BSI can be called on to help with its experience spanning a quarter of a century.

I congratulate the BSI on its 25th anniversary. Today, its existence is more important than ever before.

Dr. Wolfgang Schäuble,
Member of the Bundestag, Federal Minister of Finance

Greeting by Dr. Thomas de Maizière, Federal Minister of the Interior

Dear readers,

When the BSI was founded a quarter of a century ago, neither the incredibly rapid developments in information technology nor the challenges that they would bring with them could be foreseen as such.

However, there was a sense that digitalisation would change our lives. And in the event, it certainly has done. Today, the world is easier to grasp, people are closer to each other, and fascinating possibilities and major opportunities have been opened up.

But digital progress has not come without its risks. Networked IT doesn't just mean saving on resources and optimising processes. It also entails complexity, dependencies and hazards. Digitalisation can only succeed when at the same time, a high level of IT security is guaranteed.

That's why it was absolutely the right decision in 1991 to create an independent, expert body responsible for all areas of IT security. Today, the BSI is the central authority for IT security in Germany. At international level, too, it has earned itself an outstanding reputation and is highly respected.

The BSI will also continue to play a key role in shaping the digital future of Germany. I am aware of the high level of expertise and huge commitment among the BSI's staff – the heart of the office. My thanks on this anniversary go to them.

I am sure that the BSI is capable of handling the increasing speed of change, and that it will always be able to cope with new developments. I wish the BSI continued success on its truly successful onward journey!

Dr. Thomas de Maizière,
Member of the Bundestag, Federal Minister of the Interior

25 years of the BSI

On 16 September 2016, the official celebration of “25 years of the BSI” was held in the town hall in Bonn-Bad Godesberg. Alongside the BSI members of staff, the 400 guests included Federal Minister of the Interior Dr. Thomas de Maizière and Dr. Hans-Georg Maaßen, President of the Federal Office for the Protection of the Constitution (BfV).

25 years of the BSI – during the course of a quarter of a century, the Office has been subject to considerable changes. The increasingly rapid rate of digitalisation and the greater degree of dependence of people on information technology have made it even more important to focus on cyber security. Today, the BSI is the national cyber security authority, which plays a key role in helping shape information security in the process of digitalisation. It is the key point of contact and the leading centre of expertise when it comes to IT security for the state, for business and for society.

This point was stressed by BSI President Arne Schönbohm in his opening speech: “We have succeeded in keeping pace with the development of information technology over the last 25 years. The BSI has its staff to thank for its technical

"The future viability of German economic power depends on many factors – one of which is cyber security. We want secure channels of communication, which includes the Internet. This is important not just to the government for its internal communication, but also to businesses and to us as citizens."

***Dr. Thomas de Maizière**, Federal Minister of the Interior*

expertise, and that's what makes us such a strong force in Germany. It is important that we are knowledgeable about the past and understand the present in order to be able to shape the future. Only in this way can we offer security against cyber risks."

Federal Minister of the Interior Dr. Thomas de Maizière said in his speech that cyber crime has many faces, and that a new face appears to be added every day. Without an institution such as the BSI, digitalisation would not be protected in the long term. He added that he hoped that the BSI could present a safe face to upcoming future technologies and digital progress.

The photos on the following pages give an impression of the celebrations and the reactions of guests. **>>**

"During the 1980s, the subject of computer security took on an increasingly important role. The first step was to establish the predecessor of the BSI, a computer security division which at that time had a total staff of 60. That was a relatively large number. It very quickly emerged that computer security is not just a matter for the military and the secret services, but for society as a whole."

***Wendelin Bieser**, formerly at the Federal Ministry of the Interior*

"Overall, the challenge was to maintain an independent and neutral position when it came to information security, and in so doing, to establish an entirely new location for information security in Germany."

***Andreas Könen**, Head of the "IT and Cyber Security; Secure Information Technology" directorate in the Federal Ministry of the Interior, and former Vice-President of the Federal Office for Information Security*

"The biggest challenges were that the BSI was compiled from different authorities and people from the sciences and administration, and that it had to grow together. Naturally, everyone came with their own background, and it wasn't always easy to agree on a common line and to fill with life the key objectives in accordance with the BSI Act."

Marit Blattner-Zimmermann, *formerly at the Federal Office for Information Security*

"In the past, too little priority was given to cyber security. I am very glad that we have a strong partner in the BSI and that we have a good Cyber Response Centre. I am proud that we have taken major steps forward in terms of collaboration."

Dr. Hans-Georg Maaßen, *President of the Federal Office for the Protection of the Constitution (BfV)*

"The highlight was certainly the founding of the BSI and the passing of the first BSI Act. There was an extremely intense debate on the matter between the Federal Ministry of the Interior and the different parties in the German parliament. Specifically with the representatives of the data protection authorities, who at that time did not yet understand the difference between data protection and data security. We had tough, but ultimately very successful discussions."

Eckart Werthebach, *former state secretary of the Federal Ministry of the Interior*

"Without cyber security, there will be no digitalisation in Germany, since it is an essential basic requirement that makes it possible for our way of living together to function."

Arne Schönbohm, *President of the Federal Office for Information Security*

"We discovered that the same questions were repeatedly asked when advising public authorities. We began to write down the answers packaged as modules in a modular structure, which finally became the IT-Grundschutz with which we are familiar."

Isabel Münch, *Head of the IT-Grundschutz section, Federal Office for Information Security*

"The highlight of my time working at the BSI was making it clear in 2005 that the BSI is indeed an authority which needs to grow and develop further. Until that point, the Office staff had not been expanded since the founding years. If that hadn't changed, the BSI would not have been in a position to even remotely fulfil the tasks for which it has been designed."

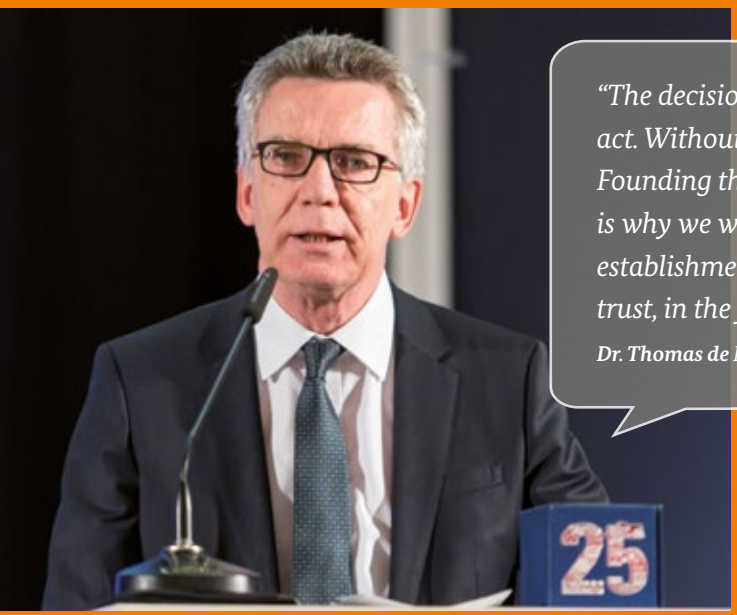
Horst Samsel, *Head of the department Consulting for Government, Private Sector and Society, Federal Office for Information Security*

"The challenge was to found the office in the first place. It happened during the period of reunification, and IT-Grundschutz was not a political focal area. It was important that this proposal put forward by parliament be put into practice. In the last session of the Federal Council, on 18 December 1990, the decision was made to found the BSI."

***Michael Hange,** former President of the Federal Office for Information Security*

"During my time at the BSI, the change to the BSI Act was made in 2009, which gave the BSI very far-reaching competencies in the commercial sector. The first challenge was to try out how this law worked. In our first case, we issued a warning about a product that was very widely distributed, and in so doing, we naturally triggered a powerful response. This had an enormous impact on the position of the BSI and also on the way the BSI was perceived, particularly in the IT sector."

***Horst Flätgen,** former Vice-President of the Federal Office for Information Security*



"The decision to found the BSI 25 years ago was a pioneering act. Without knowing exactly how this future would unfold. Founding this institution was a phenomenal step, and that is why we wish to celebrate its 25th birthday today. Since its establishment, the BIS has become a beacon, a beacon of trust, in the field of IT security"

***Dr. Thomas de Maizière,** Federal Minister of the Interior*

The BSI in dialogue

New event series begun

With “The BSI in dialogue…” the BSI has begun a new event series as a forum for discussions and information exchange with participants from the state sector, business and society. The aim is to achieve greater awareness of all topics related to digitalisation and cyber security.

The successful launch event was held in Berlin together with the BKA, the Federal Criminal Police Office. The main topic of discussion was ransomware, the threat from malware which prevents access to data and systems and only re-releases them after ransom money has been paid. The first ransomware versions and concepts were already in existence before 2000. Since 2011, ransomware has become a widely distributed form of malware. There are reports in the media about attack campaigns and new versions of this malware type almost every day, and private individuals, companies and administrative bodies are affected to the same degree.

In his opening speech, BSI President Arne Schönbohm emphasised the challenges to IT security in organisations and companies resulting from ransomware. The IT security incidents related to ransomware show how dependent we all are on information technology, and what the effects of a cyber attack can be. The programme was rounded off by two brief presentations by the BKA and the BSI about IT security measures in companies and administrative bodies, the human factor as a weak link and the impact of the IT Security Act. The event, which lasted about two hours, ended with a lively discussion among the more than 30 participants.

The BSI is taking a cooperative, regional approach with these events. The plan for the future is to continue the series in other cities together with regional and trans-regional partners of the BSI. ■

Further information:
https://www.bsi.bund.de/Veranstaltungen

CHALLENGING YEARS

by Arne Schönbohm, President of the BSI

It was at the latest when the IT Security Act was passed that the role of the BSI changed from an expert authority into an independent institution acting in the political-commercial arena. Our tasks and responsibilities were again extended. We are and still remain the central IT security service provider of the federal government and will also be providing increased support to other state organs. However, we are also the central port of call for IT security needs and digitalisation in the commercial sector and society. In particular, our collaboration with the Critical Infrastructures (KRITIS) has been entirely redefined. To put it briefly, we now also take on the role which we have played for the federal government authorities since the amendment of the BSI Act in 2009 for KRITIS operators.

The Act is not only important for the BSI, but above all reflects the increasing importance of IT security in a digitalised society. The opportunities linked to this digitalisation for Germany as an industrial location are great – but only if we are also aware of the risks that this entails and work proactively to avert them. Companies and administrative institutions must constantly adapt to IT security threats and prepare and implement measures to prevent, detect and respond to them. This is a complex process which demands time, money and personnel resources. Individual companies have already been very active in this area for many years. Others have so far done little to nothing. This applies above all to many small and medium-sized enterprises.

The positive trend of recent years is continuing: an increasing number of companies are taking cyber security more seriously. Unfortunately, this often only happens after problems have arisen. Those involved should now long be aware of the fact that the increasing networking and digitalisation in all areas of life and work cannot lead to success without IT security.

FOCUSSING ON CYBER SECURITY

For us, an important topic over the coming years will be supporting the digital agenda of the German federal government. Here, we at the BSI can make a decisive contribution towards ensuring that digitalisation is a success in Germany, through greater visibility, more dialogue and more activities.

- We are intensifying our exchange of information with the executive management and supervisory boards of the DAX and M-DAX listed companies and small and medium-sized enterprises (SMEs).
- We are increasing our contact with IT users, and are conducting meetings and establishing working groups with them.
- We issue warnings against applications with a high level of insecurity and give recommendations for security measures.
- For us, information security is a management issue.

"IT security must already be given at least equal priority alongside economic and functional factors when developing new products and services."

In the future, every company will have to have an executive digitalisation management or CDO (Chief Digital Officer), who will demonstrate to their colleagues that cyber security is a competitive factor in the process of digitalisation. Here, it is not enough simply to have a member of IT staff who is responsible for this task. That's why this year, we are above all expanding our dialogue with the decision-makers in companies, in order to convince them that IT security is an integral part of the risk management of their company, and also to make adequate provisions in areas such as Industry 4.0 or the automotive sector in particular.

IT security must already be taken into account when developing new products and services, and must be given at least equal priority to economic and functional factors. After all, our report on the situation of IT security in Germany shows that the number of weak point and vulnerable areas in IT systems remains at a very high level. The asymmetric threat level in cyberspace has escalated further. It can only be kept in check through cooperation, with the state, the commercial sector and society working together.

EXTENDING COOPERATIONS

We have created the cooperation platforms needed to do so and are continuing to extend them.

- The Alliance for Cyber Security has developed in a very positive way since it was founded. The number of partners, multipliers and participants is constantly growing (the current figure is 1,980), so that as a result, we are in a position to reach an increasing number of institutions regularly and on a long-term basis with the services provided by the Alliance.
- UP KRITIS has been making a key contribution to the reliable provision of critical services for people in Germany since it was officially launched in 2007. Here, the focus is on the effective interaction between IT security and the maintenance of critical business processes.

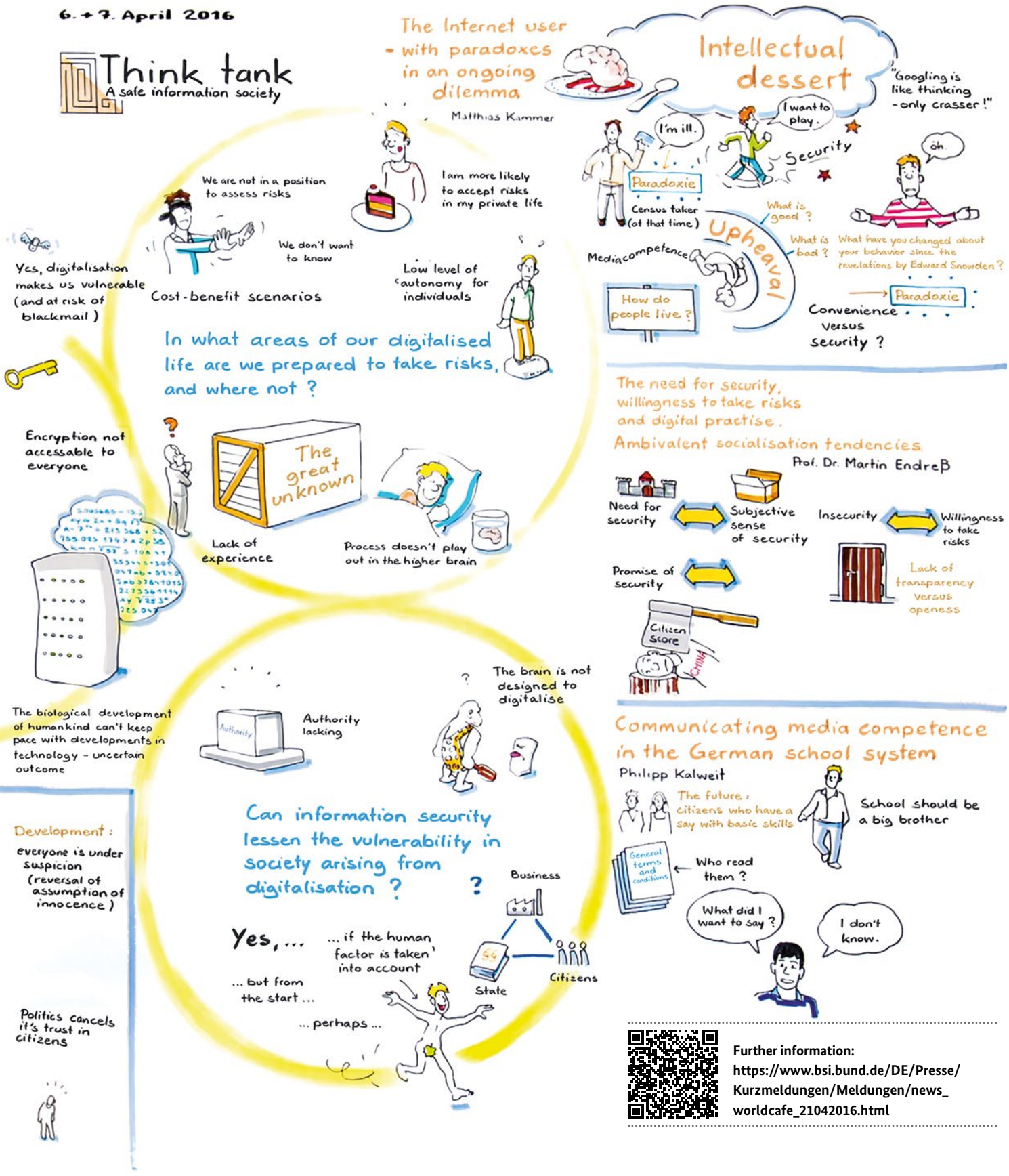
The cooperation with the commercial sector will also be an important area of work for the BSI over and above this platform in the coming years. The progress in industrial development is leading to a seemingly endless quantity of new products for the Internet of Things, Industry 4.0, Cloud or Big Data, which also entail an entirely new threat of risk. Industry is becoming increasingly dependent on IT, and its ability to function at the interfaces is regarded as being exposed to a high degree of risk. Many established mechanisms in industry have not been adapted to keep pace with digitalisation, and for many processes in networked industrial plants, the basic principle of safety before security still applies. In this area, we are already offering many specific forms of assistance and services, and will expand on these by providing further cyber security recommendations. Here, we are setting store by cooperative measures, although this does not exclude the possibility that regulatory action will be taken if necessary. At the same time, we are continuing to increase the number of certificates and are modernising the IT-Grundschutz.

For us, the focus during the years 2016/17 will be very clearly on implementing and operationalising the IT Security Act. The first section of the Decree on the Determination of Critical Infrastructures (BSI-KritisV) has been in force since the beginning of May 2016. It initially identifies Critical Infrastructures in the energy, information technology and telecommunications sectors, as well as water and food. By the beginning of 2017, with an amended decree, the aim is also to identify operators in the transport and traffic, health and finance and insurance sectors. For this reason, we must prepare ourselves quickly and well to meet these challenges, both in terms of personnel and our organisational structure.

There's one thing that won't change: progress in the area of technical defence against cyber attacks is always made step by step – a fact that is sometimes difficult to accept. However, the broader the base, in other words, the greater the awareness of the importance of IT security for all areas of our everyday life and work, which today are networked, online or digitalised, the larger these steps can be. This is what we are working to achieve. ■

Think tank for a secure information society

In April 2016, fifty representatives from civil society, the sciences, the commercial sector and public administration discussed how an information society can be made smart and at the same time secure. As a first result, seven theories were developed and passed by consensus agreement. The intense and occasionally contentious discussion was recorded by Visual Facilitators.



Further information:
https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_worldcafe_21042016.html

IT SECURITY
IN PRACTICE

“SINA was born out of the requirements for modern and at the same time secure office communication”

Interview with Dr. Rainer Baumgart

The Essen-based secunet Security Networks AG developed the Secure Inter-Network Architecture, or SINA, on behalf of the BSI. This is used to securely process, store and transmit classified documents and other sensitive data and is today being further developed on an ongoing basis by secunet. Dr. Rainer Baumgart, chairman of secunet, looked back on many years of collaboration for the BSI Magazine.

The Secure Inter-Network Architecture, or SINA, is the result of a long period of collaboration between secunet and the BSI. What makes it so special?

The BSI and secunet have in effect been working together in the area of IT security since secunet was founded. The collaboration was intensified when secunet won the first tender for the technical implementation of the SINA concept developed by the BSI. Or to put it another way: SINA was born as a result of the move by the German federal government from Bonn to Berlin and the increasing need for modern and at the same time secure office communication. A decisive factor in the success of SINA is the end-to-end security architecture. It covers different gateways, line encryptors and highly effective management through to secure clients and a tablet. For around 15 years, the components have been proving their worth among public authorities, armed forces and companies provided with confidentiality protection services, and are used by them to process and transmit classified documents – up to and including CONFIDENTIAL, NATO SECRET and SECRET EU.

SINA is being continuously further developed in close cooperation with the BSI, taking into account the particular customer requirements and strict authorisation conditions.

On what topics and areas of development of IT security are the BSI and secunet collaborating, aside from SINA?

We intersect with the BSI in nearly all areas of IT security. I would particularly like to emphasise our cooperation on issues surrounding electronic identity documents and biometry, alongside the wide range of consultancy activities with which we support various different areas of the BSI’s work. In what was still a new field at that time, real pioneering work was needed when the object was to record personal physiological features, convert them digitally and store them as electronic data records in travel and identification

Profile in brief:

Dr. Rainer Baumgart has been at secunet since 1997. He has been a member of the board of secunet Security Networks AG since 1999, and took over the chairmanship in 2001. Holding a PhD in physics, he can look back on a 25-year career in the field of IT security, which includes periods working for RWTÜV AG and TÜV Informationstechnik GmbH.

documents. The results of the numerous studies resulted in the BSI Standards, which are not only of importance at national level, but which also form the basis for international standards for electronic identity documents. Today, electronic passports are issued almost everywhere in the world which are oriented to these standards, enabling fast and reliable identification of travellers. In addition, the BSI and secunet are working with other partners on the development of automated border control systems, or eGates.

The digital world is constantly changing. How can we expect IT security to develop in the future?

The increasing degree of digitalisation is creating more risks. In the light of this extremely rapid development within IT, our task is to correctly assess the threat situation and react to it with the appropriate security technology. Here, companies and public authorities are affected to the same extent. Let's take the critical infrastructures – or KRITIS – as an example. Here, we cannot just cover the major sectors which are clearly affected, but also have to actively drive forward IT security in medium-sized enterprises and in industry in particular.

In order to be able to create up-to-date situation overviews and initiate the corresponding countermeasures if security is breached, information exchange must become institutionalised to a greater degree. Alliances such as the Alliance for Cyber Security are one way of doing this. However, we should not look at Germany in isolation, but must extend information exchange to at least the European level in order to be able to guarantee a high level of security in cooperation with all relevant stakeholders.

As well as good concepts, we above all need skilled staff in order to be able to tackle future threats. Germany is still the world leader in the area of IT security and cryptography – and this is also reflected in the wide range of activities of the members of the German professional association of IT security, TeleTrusT. This competence in the field of security is a decisive cornerstone with regard to digital sovereignty and is not least the fruit of the collaboration between the BSI, those in need of support, the federal government and the German IT security industry. One of the key challenges in the immediate future will be to obtain the right members of staff who have the necessary skills. ■

In 1999, the BSI started a project on securing IP-based networks using cryptographic securing mechanisms. Classified documents which until then had been stored in a safe and only transported by courier under the strictest secrecy were now to be transmitted via the Internet and made available for storage on PCs and laptops. The particular challenge was to secure PC systems and networks which were in principle unsafe in such a way that maximum security could be guaranteed - at a low cost and using a simple procedure.

Further information:
https://www.bsi.bund.de/SINA

Preventive concepts for tackling cyber crime

The police gives advice

Pursuing the perpetrators of criminal acts is just one way of protecting society against crime. Another is crime prevention, the concept of which aims to prevent crime from occurring in the first place. In Germany, the "Progamm Polizeiliche Kriminalprävention der Länder und des Bundes" (ProPK), the police criminal prevention programme for the federal states and the federation, has also been giving support to citizens to take action in response to criminal acts in the digital world.

The preventive concepts, initiatives and media developed by the crime prevention police authorities of the federal states and the federation are based on the desire to increase the security of the population. Key aspects are education about crime and the communication of recommended measures to protect against criminal acts. In particular, they also provide information about cyber crime and other criminal acts perpetrated through the Internet.

Their standard approach is to communicate their message using posters, flyers, radio and television. They created the slogan "When the police give advice" during their founding years and continued to use it in the decades that followed. It also lays the foundation for the crime prevention work provided by the police today. The solidarity between the federation and the federal states, which is reflected in the programme name, has proven to be a success. The product portfolio includes over 150 media. They can be ordered free of charge online, or collected from over 500 police stations authorised to issue them throughout Germany. In 2015 alone, over 4 million brochures, flyers, posters and other media were distributed among consumers and experts.

They also included numerous publications which contain information about security in everyday digital life. This has now become a key focus of preventive work. The police have adopted the approach of investigating crime via the Internet, and also naming specific criminal acts. In this way, the aim is to protect the public against falling victim to cyber criminals – but also to prevent them from becoming perpetrators themselves.

In short, the ProPK informs about crime, explains ways in which people can protect themselves and in so doing reduces the causes of crime. The focus is always on protecting the victim.

SMART LIVING –
5 TIPS TO ENSURE THAT SMART HOMES ARE ALSO SAFE

Nowadays, apps and tablets can be used to operate a whole range of devices, including washing machines, alarm systems and televisions. Thanks to digital radio transmission and the Internet, they can be accessed at all times, are constantly switched to receive signals – and also present a potential security risk. For this reason, the principle of "Internet security" also applies to smart TVs, alarm systems and other Internet-capable household appliances.

THE POLICE CRIME PREVENTION AUTHORITIES AND THE BSI RECOMMEND THE FOLLOWING MEASURES:

- Read the operating instructions carefully and make sure the special security settings have been made for Internet-capable devices.
- As a matter of principle, always change default passwords.
- Choose a password with at least twelve characters, and one that can't be found in a dictionary. It should consist of capitals and small letters in combination with numbers and symbols, and at first sight should appear to be randomly compiled.
- Make sure that the basic security measures have been taken for your Wi-Fi network. Wireless radio networks are sometimes delivered with just the minimum security level settings as default. According to the recommended Wi-Fi encryption procedure, the password should be at least 20 characters long.
- Only switch on the camera function, for example on your smart TV, when you need to use it.

BSI AND ProPK – A CONGENIAL DUO TACKLING CYBER CRIME

The success of the programme is due to clearly regulated, ongoing cooperation between the police in all federal states and to successful cooperation between the federation and the states. The central headquarters of the ProPK in Stuttgart coordinates all activities within and beyond the police committees across federal state borders. A project management group is responsible for the strategic orientation of the programme, while a federation-federal state commission (the "Kommission Polizeiliche Kriminalprävention", or commission for police crime prevention) is tasked with developing the concept.

However, their success is also due to a large number of cooperation partners, who support the police concepts and provide a valuable contribution with their specialist knowledge. The ProPK has been collaborating with the Federal Office for Information Security (BSI) for over a decade. Examples of this beneficial and necessary cooperation are the security guide, which contains the most important rules on secure Internet use, and the film "Verklickt!", which educates school pupils about the many different risks connected to the Internet. ■

"Verklickt!" Security in everyday media life - a film for pupils from year 7 and upwards.
For more information in German, go to: http://www.polizei-beratung.de/startseite-und-aktionen/verklickt.html

DIGITAL SOCIETY

Under the code of confidentiality

by Thomas Caspers, head of Evaluation and Operation of Cryptographic Systems division

No-one would ever be so rash as to send intimate details about their private lives on a postcard. The concern would be that this communication would end up in the wrong hands. In fact, however, unencrypted e-mails are no different than postcards – and on a big scale. Even so, according to a current bitkom survey, only 15% of all users in Germany send their e-mails encrypted. Astonishing when you think of the risks involved.

What they contain is only intended to be read by the addressee and remains confidential between sender and recipient. This requirement is not just a product of the recent process of digitalisation. The origins of modern crytpology methods extend far back into the history of human civilisation. It is highly probable that humans have been coding texts since the existence of writing in order to protect critical information against unauthorised access.

SECRET CODE – AN ANCIENT RECIPE

One of the first ideas here was for the sender to use characters different to those which were generally known and with which only the recipient was familiar, whose task it was to decode the message using a key. Digital coding methods also convert information to be protected into data which cannot be deciphered by unauthorised recipients – with the difference that today, encryption is an important competitive factor in Germany as a business location. After all, digitalisation can only develop its full potential for added value when the necessary security measures are taken to protect companies and citizens. For this reason, the German federal government has announced its goal of making Germany the "no. 1 encryption location". As part of this process, the government's digital agenda envisages, among other things, "the encryption of private communication among the broad general public".

WHO LOCKS WITH WHICH KEY?

In general, two encryption methods are used: symmetrical and asymmetrical. Symmetrical methods are based on the fact that the sender and the recipient use the same code for encryption and decoding. This might be simple, but it is also the weakness of this method, since for it to work, the key first has to be exchanged. If it falls into the wrong hands, the communication can be decrypted and read. For this reason, the asymmetrical method was developed. Here, different keys are used for encryption and decryption. The decryption key no longer has to be issued, making it much easier to exchange the keys. With e-mail coding, only the public portion of the key is exchanged which is needed for encryption. The second decryption key is withheld by each user, and therefore remains secret.

DIGITAL KEY HOOKS

Two different concepts have been developed to manage these keys: OpenPGP and S/MIME. The advantage of S/MIME is that it not only encrypts emails but also immediately confirms the identity of the key owner using an independent certification authority (CA). While OpenPGP does not provide such confirmation, it is available within just a few minutes and can also be used anonymously. Both approaches are equally effective when it comes to security. In the commercial world, the more sophisticated S/MIME standard is often recommended due to its additional functions, while in the private sphere, the uncomplicated OpenPGP solution is generally the preferred option.

Yet regardless of whether they choose S/MIME or OpenPGP, until now there are still only very few e-mail providers who provide end-to-end encryption right from the start.

Most large portals transport messages in an encrypted way from the customer's system to their server, and then from their server to that of another provider, but do not encrypt uninterruptedly from the sender to the recipient, the two end points of the communication. To ensure that uninterrupted e-mail encryption becomes standard practice, it should function without the user having to do anything – ideally on all platforms used today for e-mail communication, from the web browser on a PC through to the e-mail client on a smartphone.

ON THE ROAD TO BECOMING THE "NO. 1 ENCRYPTION LOCATION"

In order to promote encryption in Germany, representatives from politics, research and IT businesses have joined together and committed themselves to provide simple, transparent encryption solutions in the "Charter for strengthening trustworthy communication", led by the Federal Ministry of the Interior. These providers are making "real" end-to-end encryption available – from the sender's outbox through to the inbox of the recipient. The user only needs to activate this protection or set it up in their e-mail program. This is being followed by further initiatives such as the "people's encryption" – alliances which the BSI welcomes. The public authority lays the foundation with technical guidelines and expert specifications, on which the encryption solutions offered for guaranteeing secure encryption according to the latest technological standards can be built. It informs companies and private users about how they can quickly and effectively protect their e-mail communication using simple tools. ■

THE BSI SOLUTION: Gpg4win

With Gpg4win, the BSI is offering its own licence cost-free encryption solution for Windows operating systems, with which any user can encrypt and decode e-mails, files or folders in a simple way and free of charge. The source code for this solution can be set by anyone, allowing its functioning to be monitored independently of the BSI. Furthermore, with Gpg4win, the integrity (unchanged nature) and origins (authenticity) can be secured and checked using digital signatures.

Further information:
https://www.bsi.bund.de/Gpg4win

“With the discovery of Gameover Zeus, we have written cyber crime history”

Interview with Prof. Dr. Christian Rossow

The information technology expert Prof. Dr. Christian Rossow researches malware and finds “Gameover Zeus”, a malware which has been used by cyber criminals to steal over a hundred million dollars in total. Through a weak point in the code, Rossow smuggled himself into the botnet of the criminals and rendered it harmless. The BSI Magazine interviewed him about his work.

How did you discover Yevgeni Bogachov’s Trojan?

For years, malware has been a major focus of my research work. To be able to tackle the daily flood of malware, we have researched an analysis environment specifically for malware at our institute, in which we can observe the behaviour of the viruses. The principle is similar to that of a test tube in a biological virus laboratory. We deliberately infect virtual machines with malware in order to observe what actions it takes. In this way, we can see how the malware embeds itself in the system, which processes it manipulates, what data is stolen and also what communication is made with the attacker. We became aware of “Gameover Zeus” in this analysis environment since the Trojan established an unusually large number of outgoing communication connections.

When did you know what kind of fish you had at the end of your line?

Many months passed before we conducted a detailed analysis of the malware and realised that we had discovered a real Trojan. We formed a research group with the involvement of companies such as Crowdstrike and other universities such as the VU Amsterdam and the University of Bonn in order to analyse Gameover Zeus using “reverse engineering” techniques. This process is often highly complex, since you have to be able to make conclusions about the entire semantics of what is an extremely intricate program on the basis of just the machine code. When we discovered the technical details of the Trojan, we could see that it was a large and relevant botnet. However, at the latest when the FBI contacted us from the US to ask us to cooperate in fighting the Trojan, we realised that we would write a major chapter in the history of cyber crime.

How did you manage to stop it?

For the first time, we were afraid that we were confronted with a malware which we would not be able to “hobble”. A large number of botnets are relatively easy to eliminate by shutting down the central command server. However, Gameover Zeus uses a decentralised communication structure with no so-called “single point of failure”. In other words, even if we had shut down individual systems, the botnet would have been able to continue operating normally thanks to its peer-to-peer technology.

Profile in brief:

Prof. Dr. Christian Rossow, Professor for IT-Grundschutz and head of the "System Security" research group at the Center for IT-Security, Privacy and Accountability (CISPA) at the University of Saarland.

This was the starting point of our research. We researched new methods in order to manipulate the decentralised communication of the network in such a way that the individual bots, in other words, the infected systems, lost their contact with the other participants in the network. After we tested several prototypical attacks on the botnet, we became sure that the network could be technically incapacitated. This was then done in a joint operation with the FBI in June 2014, while the FBI simultaneously pursued the people behind the malware.

Is there such as thing as the perfect code?

If there were such a thing as an entirely error-free code, then some IT security problems would be resolved. However, experience shows that even software which is subject to the highest industry standards continues to contain weak points. It's not for nothing that many administrators the world over are concerned about safety-critical updates which they have to install as quickly and completely as possible on their systems. In the research field, we are therefore concerned both with methods to detect weak points and in so doing to also make it harder to exploit them.

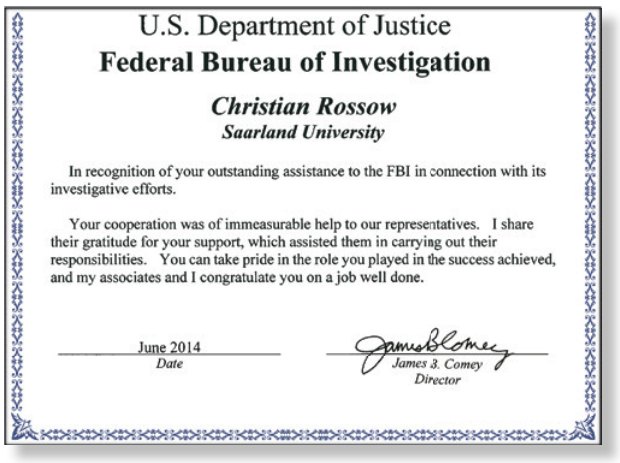
With regard to Gameover Zeus, we can say that the weak points exploited by us for the attack on the botnet could in principle be closed. Peer-to-peer botnets such as Gameover Zeus are relatively complex and therefore also prone to error. Even so, it is feasible that in the future, we will encounter indestructible decentralised botnets.

How can the battle against cyber attacks with viruses, Trojans and the like be won? What should companies and members of the general public expect to see in the future?

Malware has been known for over 30 years, and we are still – or indeed in today's world more than ever before – looking to find suitable countermeasures. Unfortunately, attacks are becoming increasingly sophisticated. One current mass phenomenon, for example, is ransomware, which blackmails its victims into paying money before re-releasing locked systems or coded files.

Alongside malware designed to create mass damage, which infects millions of systems worldwide, we are also seeing an increase in targeted and politically motivated attacks. These attacks are much harder to detect, since the attackers first spy out information on potential victims using social engineering in order to then reach the target individuals with a higher degree of probability. On the other hand, it is only possible to detect targeted attacks in very few places, with the result that they have a better chance of being conducted unrecognised in the background.

Dr. Rossow, thank you for talking to us.



U.S. Department of Justice
Federal Bureau of Investigation

Christian Rossow
Saarland University

In recognition of your outstanding assistance to the FBI in connection with its investigative efforts.

Your cooperation was of immeasurable help to our representatives. I share their gratitude for your support, which assisted them in carrying out their responsibilities. You can take pride in the role you played in the success achieved, and my associates and I congratulate you on a job well done.

June 2014
Date

James B Comey
James 3. Comey
Director

FBI certificate awarded to Prof. Dr. Christian Rossow

IT SECURITY IN INDUSTRY 4.0

by Dr. Christian Haas, head of the "Secure networked systems" research group at the Fraunhofer IOSB

Profile in brief:

Dr. Christian Haas has worked for the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) since 2015 and heads the "Secure networked systems" research group there. He studied information technology at the Karlsruhe Institute of Technology and earned his PhD there at the Institute of Telematics under Prof. Zitterbart, with a focus on evaluating the energy efficiency of security mechanisms in wireless sensor networks. The "Secure networked systems" group focuses mainly on research and development topics in the area of security for industrial production and critical infrastructures.

Suitable test environments are essential

Today's production plants are very highly networked. Controls and embedded systems communicate independently with each other, while planning systems from the Cloud calculate order fulfilment steps and machine deployment, plant managers use remote monitoring and control measures, and maintenance staff access systems worldwide and make configuration changes. Appropriate measures are essential to provide protection against damage or production outages arising from breaches of security. IT security in the sense of security against attacks is one of the aspects most critical to success, and must be developed and ensured as a precondition for well-functioning, comprehensive Industry 4.0 solutions.

For some time now, open standards (such as the IEC 62443) and solutions have been in existence which offer procedures and technical solutions to operators of production plants or manufacturers of components and systems so that they can develop and implement appropriate security measures. Even so, everyday work in modern production plants shows that in many cases, almost no security measures have been implemented, or those that are in place are not consistently used. This is often the result of the crossover between different areas of responsibility, such as IT (Information Technology) and OT (Operational Technology), as well as the lack of suitable testing and training environments in order to become familiar with existing security measures and try them out.

In order to assist companies in tackling these problems, the Fraunhofer IOSB has developed an ideal test environment with its IT security laboratory, where it replicates real-life production scenarios, tests security measures and studies the effects of attacks. The IT security laboratory, which is specifically equipped for production and automation technology, offers a secure environment in which the entire hierarchical IT infrastructure of a factory with office network and networks for production planning, monitoring and control can be reproduced. This reality-based IT network environment is partially structured from typical industrial network elements and as a virtual network structure in a Cloud. In the IT security laboratory, we work among other things on further developing tools and security mechanisms specifically designed for industrial production environments. The equipment in the IT security laboratory is also used for training and education purposes, for example as part of training events, to demonstrate how IT security can already be implemented for Industry 4.0 using the IT security mechanisms available today. ■

Certainly no job like any other.

Germany's most attractive employers 2016
TOP 100
trendence GRADUATES

We're looking for you! www.bsi.bund.de/jobs

LEGAL NOTICE

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

Source: Federal Office for Information Security (BSI)
Section B23 – Public and Press Relations
Godesberger Allee 185–189
53175 Bonn, Germany
Phone: +49 (0) 22899 9582-0
Email: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de

Last updated: September 2016

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

Concept, editing and design: Fink & Fuchs Public Relations AG (FFPR)
Berliner Straße 164
65205 Wiesbaden
Internet: www.ffpr.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 16/704-2e

Image credits: Title: Mopic/fotolia, silvertiger/depositphotos; p. 1: Stephan Kohzer/BSI,
p. 4: Matthias Gärtner/BSI (top left), ENISA (top right), trendence Graduate Barometer (below left);
p. 5: Federal IT Steering Unit (FITSU), Switzerland (above left), CSCG (below right);
p. 6-7: NürnbergMesse; p. 8: blobbotronic/fotolia; p. 9: LOGO eIDAS; p. 10: blobbotronic/fotolia;
p. 11: ANSSI (above), R.Winkler; p. 12: ANSSI/Picturetank-Gaillardin; p. 13–14: R. Winkler;
p. 16–17: R. Winkler; p. 18: BSI; p. 19: Stephan Kohzer/BSI; p. 21: BSI; p. 22: Stephan Kohzer/BSI;
p. 24: Stephan Kohzer/BSI; National Cyber Response Centre; p. 26: Ilja C. Hendel/BMF;
p. 27: Henning Schacht/BMI; p. 28–33: Johannes Dominik Weber; p. 34–35;
p. 36: Stephan Kohzer/BSI; p. 38–39: Marcus Frey/VISUAL FACILITATORS;
p. 41: secunet Security Networks AG; p. 42: ProPK; p. 43: Herrndorff/fotolia;
p. 45: gst/shutterstock; p. 47: Prof. Dr. Christian Rossow,
p. 48-49: Fraunhofer Institute of Optronics, System Technologies and Image
Exploitation IOSB (below left); Dr. Christian Haas (top right); p. 50: topseller/shutterstock.

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

www.bsi.bund.de