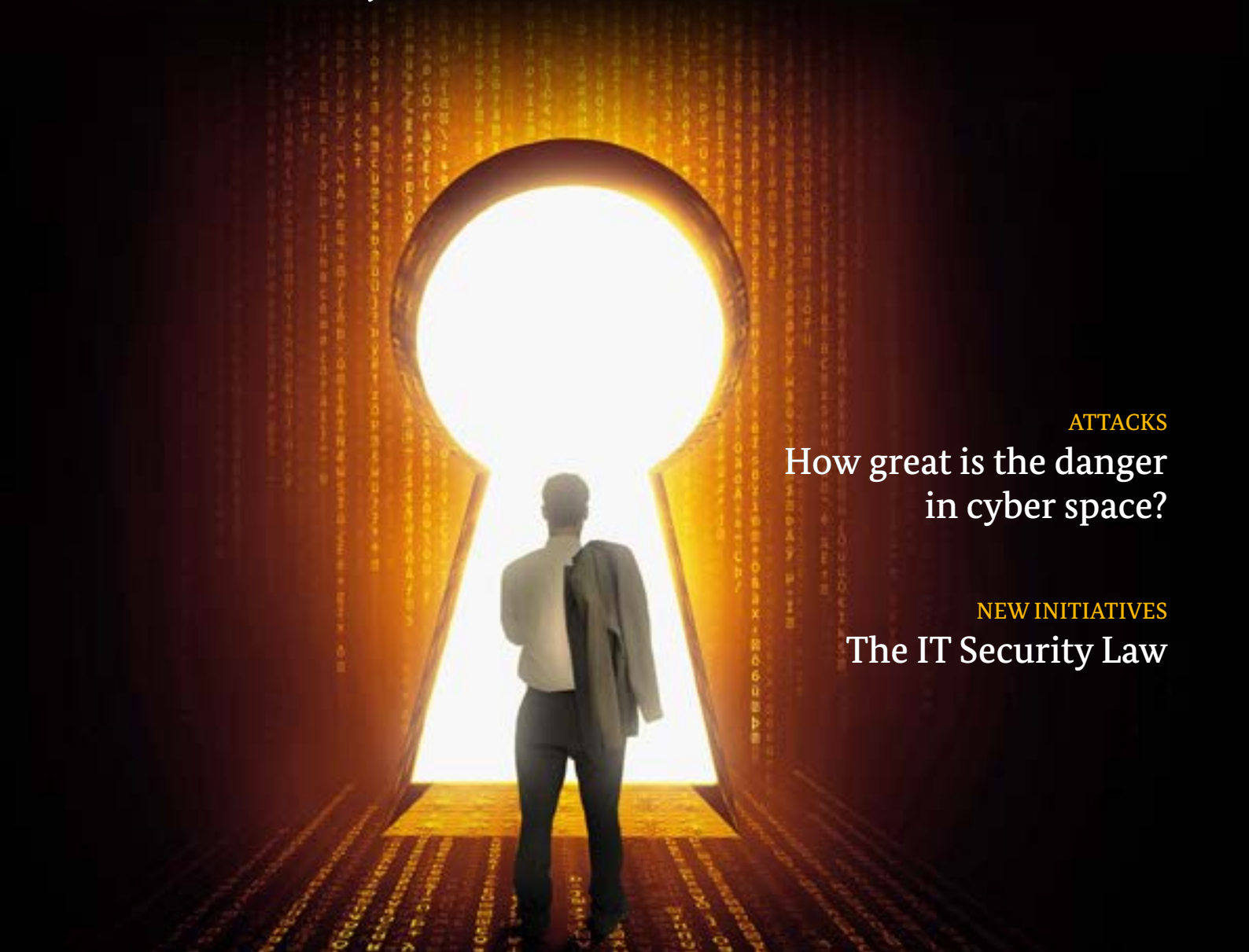
Federal Office
for Information Security

Security in focus

BSI Magazine 2013/14

Information Security

for the state, businesses and citizens



ATTACKS

How great is the danger in cyber space?

NEW INITIATIVES

The IT Security Law

Contents

Imprint

Issuer: Federal Office for Information Security– BSI, 53175 Bonn

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

Project management: Stephan Kohzer

Date: October 2014

Texts and compilation:
Federal Office for Information Security – BSI

Concept, compilation and design:
media consulta Corporate Publishing GmbH, Wassergasse 3, 10179 Berlin

Picture credits: Title: WavebreakmediaMicro/Fotolia; p. 2: T. Linack/Fotolia (t.l.), BSI (b.), Immanuel Giel (t. r.); p. 3: BSI; p. 4: jesussanz/Fotolia; p. 6: Julien Eichinger/Fotolia; p. 8: jesussanz/Fotolia (l.), BDI (r.); p. 10/11: Julien Eichinger/Fotolia; p. 11: BSI; p. 12: vinzstudio/Fotolia; p. 14, 16: peshkova/Fotolia; p. 15: FKIE; p. 17: BSI; p. 18: Bespaliy/Shutterstock; p. 19: vege/Fotolia (t.), BDI (b.); p. 21: vege/Fotolia (b.), Rohde & Schwarz SIT (t. r.); p. 22/23: Julien Eichinger/Fotolia; p. 23: BSI; p. 24: Julien Eichinger/Fotolia (t.), BMI (b.); p. 26: adimas/Fotolia (t.), djama/Fotolia (b.); p. 28: Tomnamon/Fotolia (l.), lanlanlaaa/Fotolia (r.); p. 29: floral_set/Fotolia (t.), gematik (b.); p. 30: robu_s/Fotolia; p. 31: robu_s/Fotolia (t.), BSI (b.); p. 32: Coloures-pic/Fotolia; p. 33: BSI; p. 34/35: Daniel Coulmann/Fotolia; p. 35: BSI; p. 36: weseetheworld/Fotolia; p. 37, 38, 39: Mirscho/Fotolia; p. 38: BSI (b.); p. 39: Coloures-pic/Fotolia; p. 41: BSI; p. 43, 44: Kirill_M/Fotolia; p. 45: BSI (b.); p. 47: Thorsten Schier/Fotolia (t.), BSI (r.); p. 48: Bundesregierung/Bergmann, Guido; p. 50: BSI (l.), eyetronic/Fotolia (r.); p. 51: BSI (r.); p. 53: MichaelJay/Thinkstock, BfDI; p. 54: Wolkenkratzer; p. 55: BSI; p. 56: WavebreakMediaMicro/Fotolia; p. 57: BSI; p. 58/59: Bloomua/Shutterstock; p. 60: BSI (t., m. l., m. r.); p. 61: Sven Hoppe/Fotolia (t.); p. 62: qoqazian/Fotolia (t.), Deutscher Bundestag/Achim Melde (m. l.), Deutsche Messe (m. r.), Stefan Didam (b. l.); p. 63: lohner63/Fotolia

Print: Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 63086 Frankfurt a.M., Internet: www.zarbock.de

Order number: BSI-Mag 14/701e

This magazine is a BSI public relations publication.
It is provided free of charge and not intended for sale.

Editorial

Dear readers,
Awareness of the topic of IT security has been heightened by recent security incidents, including millions of cases of identity theft online and Edward Snowden's revelations. Users – whether in businesses, in public authorities or as private citizens – have realised just how susceptible to attack IT infrastructure can be and how carefully sensitive information must be treated online.

The increasing digitisation and networking of all areas of life and work, as well as an often insufficiently protected IT security infrastructure, offer criminals plenty of opportunity for attack. It is undisputed that cyber attacks with the aim of gaining information or financial benefits take place around the clock in Germany. Government agencies, commercial enterprises and citizens are all affected.

To counter these attacks, it is important for each group to be aware of its responsibilities. We need solutions that make the use of security products practical in everyday life. We need to learn to handle information consciously and cautiously. But the creation of appropriate conditions – from a common definition of safety standards to possible IT security legislation – also plays an important role.

The Federal Office for Information Security (BSI), which currently has around 600 employees, is an independent and neutral body for all issues regarding IT security in our information society. As such, it is closely involved in the development of the necessary processes and solutions. This magazine offers insight into the various areas of our work and information on selected BSI projects.

I hope you find the magazine proves informative and thought-provoking on the subject of IT security.

Bonn, October 2014

Michael Hange
President of the Federal Office for Information Security (BSI)

Lessons learnt in recent years

Competence and trust are essential to IT security

After the loss of confidence in IT security, new precautions are needed. What can be achieved politically? What is the role of the individual?

In its infancy, the internet connected only a limited number of users: in the late 1960s it was merely a computer network of universities and research institutions. Funding from the US Department of Defense brought momentum to its expansion, but only since the 1990s have we known the internet as a global network. These days, the spread of IT technology and the resulting level of interconnection serve to further the digitisation of our world. These developments and the current forms of usage were not originally foreseen. The internet was mainly planned in terms of high availability. IT security by design – the preemptive inclusion of information security features – was not intended. Avoiding the use of cryptography has meant that data confidentiality and integrity continue to be insufficiently guarded. These design flaws are the reason for some of the most significant challenges to modern society and provide the methodological approach for many cyber attacks. A high degree of anonymity, low probability of being discovered, and lack of IT security awareness in society play into the hands of cyber criminals and promote the exploitation of this vulnerability.

IT security – where do we stand?

Germany is permanently exposed to cyber attacks with the aim of gaining financial advantage or information. Everyone is affected – public institutions, businesses and citizens. The revelations former NSA employee ›

Edward Snowden made about the methods and activities of foreign intelligence services in 2013 and IT security incidents (such as millions of cases of identity theft at the beginning of 2014) have contributed to heightening public awareness of the subject of IT security. The fact that state agencies monitor communication is not new. However, the professionalism, extent and density of monitoring activities surprised even the experts, as did the significant allocation of resources, both human and financial. Back doors in IT products are a way to break into IT systems. Known but unsolved vulnerabilities (let alone as yet unknown zero-day exploits vulnerabilities) present opportunities for the effective invasion of IT systems when not taken care of in time.

In view of this, the question arises of how to provide for the protection of privacy and confidentiality. Confidence in personal (cyber) security has suffered, but so has that in IT companies, which – according to Snowden – partially cooperate with the secret services.

Creating obstacles

The good news is that in terms of quality about 80–90 % of cyber attacks can be averted with known standard security measures. However, purely preventive measures are only one component in the process of gaining control of exposure levels. Consistent prosecution where criminal activity is concerned and careful observation of the activities of foreign intelligence services are also of great importance. This strategy must be accompanied by the creation of parameters, ranging from common definitions of security standards to possible IT security legislation. The fact that these decisions must strike a balance between privacy and public safety, between the protective function of the state and individual responsibility, between state regulation and self-regulation of the market, makes them into a challenge for society as a whole. It cannot be solved by one social group alone but requires intensive cooperation at all levels of government, industry and society.

Businesses and citizens retain the primary responsibility for their own IT security. Through its service offers, recommendations and collaboration, the BSI helps them help themselves. A good and successful example is the Alliance for Cyber Security, a national platform of cooperation that provides recommendations, good practices and solutions to over 1,000 companies and individual members, with the aim of improving cyber security in Germany.

Wherever cooperation and self-interest are not sufficient to establish an adequate level of protection, regulatory requirements should be considered. This particularly applies to facilities essential to society, the so-called critical infrastructures. From an IT security point of view, the BSI has defined a number of key actions that lead to the improvement of risk levels in cyber space (see illustration on page 7).

Six-Point Plan

Measures for all target groups

1

Promoting the use of trustworthy crypto-technology

This includes the implementation of licensed cryptographic algorithms by trusted manufacturers but also increasing the demand for already licensed crypto products (e.g. crypto phones, laptops and tablets).

2

Identifying trustworthy manufacturers and products

Measures must be taken to better guarantee transparency, as it otherwise becomes difficult to verify standards of security, confidentiality, integrity, data security and data protection. Requiring certification can act as a measure to increase transparency.

3

Technological sovereignty

In the cyber age, technological sovereignty is a pillar of national sovereignty as a whole. Worthwhile regulatory security requirements are intended to increase demand for security products, promote research and - in consequence - establish a self-sustaining IT industry in Germany.

4

Supporting citizens

Citizens must receive direct, comprehensive information about secure ways to use information and telecommunication technologies – and be warned about the risks. Cryptographic anchors of confidence (e.g. the new ID card) must be established. IT staff are encouraged to do more for their customers' safety by providing secure encryption and authentication.

5

Target group: industry

Strengthening cooperation (Alliance for Cyber Security, UP KRITIS), exchanging experience and information, recommending good practice and solutions. Promoting industry expertise through certification of IT security services. Wherever collaboration remains insufficient, the state should exercise its regulatory function (IT Security Act for KRITIS).

6

Standardisation and certification

Standardisation is an outstanding tool for establishing interoperability and security demands on modern IT systems and IT services. Standards serve to unify and enforce the objectives of information and cyber security. Certification makes it possible to meet the demand for protective IT services, for example by certifying trustworthy and competent IT security services providers.

Anchoring confidence

In future it will be important to satisfy the increased interest in security issues and to provide a wide range of practical, easy-to-use security products and trustworthy sources of information. Establishing trust will play a fundamental role, for which knowledge of functioning IT security systems will be indispensable. Trust in the actors is essential – whether they are government agencies, manufacturers or service providers.

As an independent and neutral body for all questions about security in the information society, the Federal Office for Information Security (BSI) is one such anchor of confidence. Through our expertise, neutrality in competition and our cooperation with industry and science, we continue our work to do justice to this claim. One thing is clear: IT security and the location advantage of IT security in Germany is not an individual but a common achievement.

Ultimately, recent security incidents and the Snowden revelations have facilitated an important development: they helped make society more aware of the issue of IT security and recognise its value as an important commodity. Everyone can and must contribute to the collective effort of increasing cyber security. The BSI will, of course, continue to provide full support and assistance.

Michael Hange,
President of the Federal Office
for Information Security

Dr Thomas de Maizière,
Federal Minister of the Interior

"Security and Freedom Online"

Mr de Maizière, you have made the topic of "IT and Internet Security" a central theme of your work at the Ministry. What are the key opportunities and risks involved in digitisation and how would you characterise the role of IT security?

The grand coalition has accorded IT security and the protection of citizens online a prominent position in its coalition agreement. Among other tasks, this involves the strengthening of national technological competences in the European network, the promotion of a trustworthy IT and network structure as well as support for a legal framework for data protection at European level.

The internet and related communication technologies are essential component technologies for our information society. This central infrastructure has changed how we communicate, process information and perform international business transactions profoundly – and for the better. Most processes and tasks in businesses and administrative bodies are now completed with the support of IT programmes. We are highly dependent on functioning information technology and secure information infrastruc tures. Safeguarding security in cyber space and protecting critical infrastructures are therefore essential tasks that require strong commitment by all stakeholders.

In August 2014, the cabinet adopted the Digital Agenda. What are the Agenda's key objectives? And which goals do you personally think are the most important?

Three ministers were involved in jointly presenting the Digital Agenda: the Federal Minister for Economic Affairs and Energy, the Federal Minister for Transport and Digital Infrastructure and the Federal Minister of the Interior. This procedure alone gives an indication of its scope. Working together with all social groups, we hope to find comprehensive solutions to numerous issues concerning digitisation. Generally speaking, the digital agenda has three core objectives. Firstly, our country's innovation potential for further growth and employment needs to be expanded and better exploited. Secondly, the construction of comprehensive coverage of high-speed networks and the promotion for digital media literacy competences should be supported for all generations, so that every member of society has full access and can actively participate. Thirdly, the safety of IT systems and services should be improved in order to instil society and businesses with greater confidence in online security. I see internet freedom and online security as two sides of a coin. We must make the most of the opportunity for a broad, inclusive dialogue to explore how both aspects can be reconciled in the context of the increasing digitisation of our lives.

One of the first measures proposed to implement the Digital Agenda is the draft IT Security Act, which discusses the protection of critical infrastructure, amongst other issues. What is your motivation for the bill?

Attacks on information systems are becoming increasingly well-targeted and technologically ever more complex. At the same time, we must take note of the fact that effective protection of IT systems from attacks is not yet equally guaranteed across all areas central to the functioning of our society. Due to the high degree of interconnection between the various operators of critical infrastructures, this state of affairs is no longer acceptable. That is where the IT Security Act comes into play, as it includes the introduction of mandatory minimum standards for the IT security systems of critical infrastructures, as well as the requirement to report significant IT security incidents. The BSI will play a central role in the development and recognition of these minimum standards. In addition, the BSI will inform operators of critical infrastructures about attacks and provide advice regarding the security of their IT systems. With the introduction of the IT Security Law, the BSI will also be in charge of new tasks in further areas.

Citizens often find it difficult to protect themselves against increasingly professional attackers and threats online. How can the BMI and politicians support citizens in this regard?

Personal data require secure encryption. This ensures that the data can only read by their intended recipient. One of the goals set by the government in its Digital Agenda is to make the encryption of private communications a standard procedure across the board.

In De-Mail, we already have a good and safe system for electronic communications at our disposal. The providers of the De-Mail service are responsible for the security and encryption of the data being sent and ensure that the identity of the correspondents can be reliably established. They are also responsible for registering and demonstrating the punctual receipt of unchanged documents by the recipient. The BSI regularly reviews the De-Mail system's compliance with the high safety standards. A joint working group with industry experts has been established to accelerate the comprehensive introduction of De-Mail.

It is also important to replace the use of insecure access methods like passwords with secure authentication mechanisms, such as the identity card's new eID function. Public authorities and companies that enable use of the eID function help this transition by signalling that they attach great importance to trustworthy electronic services and the protection of citizens' data. The more applications are available for the eID function, the more often citizens can benefit from the protection it offers. We are therefore committed to further expanding the range of eID function applications. We are also facilitating the use of eID by introducing new user-friendly software for the online identification card.

Besides the steps taken by the government in the scope of the Digital Agenda and the continued development of information technology by industry and science, the task of convincing the public of the need for information protection and raising awareness of the options available to each individual is integral to our efforts towards greater data protection and online security.

The German Society for Online Security (DsiN) delivers a very valuable contribution by working in collaboration with its target groups – citizens, small and medium enterprises and multipliers – throughout its various projects.

And finally: Where do you see the BSI in five years' time?

The development of the BSI will receive fresh momentum through the implementation of the IT Security Act. The aim is to establish the BSI as an international knowledge centre for the security of information technology and as a focal point for the IT security of critical infrastructures. The BSI will be equipped with powers to investigate all products available on the market, to assess them in terms of safety and to publish the results. In the next few years, the BSI will become even more established as the central institution for security in information technology across Germany.

Digital Autonomy

Information security online

Staying unobserved and independent online – how can we achieve "digital autonomy"?

The progressive digitisation of the whole spectrum of human life and economic activity – from written and verbal communication, via automotive technology, machinery and energy to medical technology – means that essential activities in all aspects of private life are subject to technological advances. In combination with the rapid and comprehensive linking-up of the underlying information technology, this development has given rise to the much-quoted "Internet of Things".

At the same time, every single piece of digital information in this network is subject to a completely new kind and level of exposure: whereas a letter used to be transmitted by a limited number of post offices (!), or a request for communication was handled by a clearly defined chain of central offices (!), the infrastructure of today's communication networks remains largely obscure to the user. Since the advent of the now ubiquitous Smartphone, this level of exposure has extended to the user's location and every aspect of their digital and online life. As demonstrated throughout this annual report, this (new) internet facilitates exposure to a great variety of security threats – be they intelligence-led or criminally motivated. There is, however, a set of characteristics common to all security threats: they target the confidentiality and availability of data and communications; aim to overcome the protective mechanisms of any IT-systems in place and – widely seen as the defining insight of the Snowden revelations – target the individual's personal online presence.

Independent and unobserved

The insight has drawn widespread demands for "independence and non-surveillance" online, involving end-to-end encryption, anonymisation, Schengen-routing and technological sovereignty. Ideas for progress in this area aim to establish a clear sense of the control, locality and ownership of data and communications as well as comprehensive knowledge concerning the infrastructure, IT products and services used, and information security. That is the goal to be pursued: a state I would like to term "digital autonomy".

A conflict of aims

"Digital autonomy", in this wide-ranging sense, is inherently burdened with a host of conflicting aims. Just a few of these are listed here:

- In many cases, users voluntarily choose to expose their personal data (e.g. through a Google search or on Facebook), thereby "paying" for the (otherwise free) services offered;
- Encrypted channels of communication can be used to shield the malicious software they transmit, facilitating illegal activities online;
- For many products nowadays, heightened security comes at the price of decreased usability.

Making "digital autonomy" a reality will involve solving a number of complex technological challenges. Sophisticated cryptography may well serve to protect confidentiality – but the goal must be transparent usability and the prevalence of an appropriate infrastructure of trust. Cyber security measures are already available – but in the face of the immense number of weaknesses in hardware and software and the high success rate of cyber attacks, the concepts of security by design and security by default must become the norm.

Protecting the individual's personal online presence poses the greatest challenge: far-reaching, structural changes to the current web and its architecture are needed to achieve a fundamental improvement of the security situation online. Progress can be made only through international collaboration in research, development and standardisation. Until then, awareness-raising and education about security risks will remain the primary method of protecting individuals online.

What measures is the Federal Office for Information Security implementing?

It is the task of the state and its institutions to create trust through transparency. This is primarily achieved by:

- Making standardised cryptographic and cyber-mechanisms publically available;
- Identifying and promoting trustworthy producers, products and services, encouraging international efforts for a secure global network infrastructure;
- And, primarily, by facilitating public discourse on the conflicting societal aims of "digital autonomy". ◻

Andreas Könen,
Vice-president of the
Federal Office for
Information Security (BSI)

How great is the threat to German cyber space?

Every day,
2 000–3 000
attacks on German government networks are registered, 3–5 of them are targeted.

1.7 million
new mobile malwares on android (2013) – increasing at a rate of 250 000 a month.

Tools for cyber attacks cost only
5 USD
per hour.

One in 40 websites is infected.

Tampered advertising banners spread 500 000 drive-by-exploits a day. A computer can become infected by merely visiting such a website.

BSI

100 000 people subscribe to Bürger CERT to receive information.

The BSI's warning and information service sends out
100 recommendations and
200 news items a month.

On average, it takes **243 days** to discover Advanced Persistant Threats (targeted cyber espionage).

Cyber crime

Bringing light into darkness

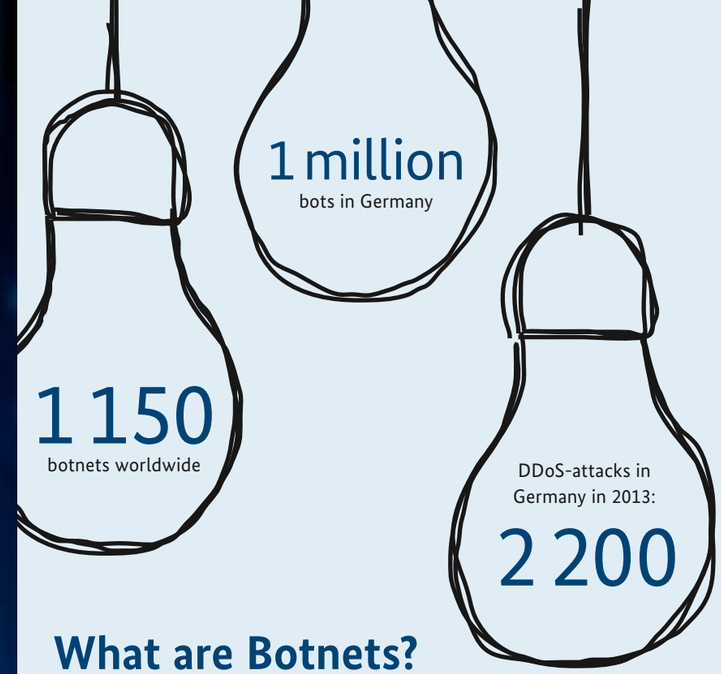
In recent years, cyber crime has become a significant problem. But how great is the danger? And how can research help?

Due to a high occurrence of unreported cases, the actual extent of cyber crime remains unknown but widely reported individual cases give an idea of the enormous scale of the damage. Overall, the investigation and prosecution of criminals in cyber space is proving extremely difficult. In addition to the technical complexity and multinational dimension of the phenomenon, the different legal systems operating in affected countries contribute to the complexity of the problem. As part of the "BOTMAN© activities" (BOTnet & Malware ANalysis), researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) are developing processes and tech nical solutions in order to tackle the phenomenon of cyber crime. These processes were defined in order for project teams to cooperatively analyse malware and investigate criminal infrastructures. Technical tools have been specifically designed for this process and facilitate the efficient analysis of malware and the design and testing of counter-measures as well as warning those affected, investigating offenses already committed and recording leads on perpetrators.

Prof. Dr Peter Martini, Director of the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE)

Dr Elmar Gerhards-Padilla, Head of Research Group "Cyber Analysis" (FKIE)

BSI MAGAZINE 2013/14



What are Botnets?

Botnets are networks of compromised systems (bots), which cyber criminals can control remotely. Information theft, spamming, Distributed-Denial-of-Service attacks (DDoS), Bitcoin mining and the targeted spreading of further malware on bots are just some of the purposes for which Botnets are used by criminals.

Other components of criminal infrastructures include specialised servers for the delivery of malicious software, systems ensuring the anonymity of perpetrators and systems managing the interaction of accomplices and cash flows. Regarding anonymisation in particular, criminals often employ a whole chain of systems to make the detection of identities as complicated as possible.

Damage caused by cyber crime

500 million

US dollars worth of damages (to individuals) caused by online banking Trojans, Citadel in 2013 worldwide (Source: Microsoft)

1.1 million

US dollars annual revenue for operators of the worldwide malicious network Bamital between 2009 and 2013 (Source: Symantec)

42.5 million

EUR* total damages caused by cyber crime in Germany in 2012 (Source: BKA)

* Figure covers reported offences only, the estimated rate of unreported offences remains high

INTERVIEW

“STRUGGLING AGAINST THE INNER SHOPKEEPER”

Dr Günther Welsch,
Head of Division
“Coordination and Governance”

How has the public’s perception of security issues changed in the wake of the Snowden revelations?

Companies, organisations and authorities are now more prepared to critically question and examine their current and previous actions in light of IT security criteria. For example, the BMI (Federal Ministry of the Interior) will take special care to use the IT services of trustworthy contractors in future. Citizens should become aware that there is a lot they themselves can do to promote their own IT security and the protection of their data. Every additional security measure makes it harder for cyber criminals to access and abuse IT systems and data.

What developments will people have to face in future?

Interconnection is now increasing at an exponential pace. Today’s digital infrastructure would have seemed utopian 30 years ago. The “internet of things”, the “factory of the future” and the seamless interconnection of information and systems in all areas of life are becoming our constant companions in this fully digital world. We are facing huge transformations in both the industrial economy and civil society.

What about the economic perspective?

The question of who can manage the transposition of conventional economic and industrial areas into the digital age most successfully has become the new global race. This is the challenge that will determine Germany’s future. Our strength currently lies in traditional industrial areas. But IT companies are leading a major economic innovation and greatly influencing our core competencies. Digitisation offers the chance to create new, dynamic business models and in future traditional industrial products will differentiate themselves by the added value they bring in the areas of digitisation and interconnection. If we want to compete on a global scale, we must integrate cyber technologies in a fast, functional and convincing way, especially with regard to robust IT security. Germany has a strong engineering sector and great expertise in IT security. We have to make them count to our advantage.

What are the key topics to be examined in the next few years?

We need to promote IT systems and online IT business models with a higher level of inherent IT security. It will be necessary to stimulate demand in this area. Significant improvements can only be expected once IT security is perceived as a real advantage in product competition.

As long as our “inner shopkeeper” tells us that the cheaper device is preferable to the one that offers more security, but is also more expensive and less ergonomic, the market will not change. In this respect, the BSI’s task is to raise awareness of the issue and, in cooperation with interested companies, to demonstrate that products with a good level of functionality can also be secure.

“EVERYONE IS RESPONSIBLE”

Dr Dirk Häger,
Head of Division
“Operational Network Defence”

Who bears which responsibilities in the fight against cyber threats?

As a society, we need to equip children, adolescents and adults with media skills. Each person bears the responsibility and duty to protect themselves as well as possible within their technical means. This principle applies all the more to operators of critical IT infrastructures and manufacturers of IT systems. In future we must be able to develop IT systems with significantly fewer weaknesses and vulnerabilities, as these are still the main source of harmful activity online. Should market forces not adequately regulate IT security requirements, the state will have to set minimum levels. It will also have to consistently pursue criminal activity online. In our globalised world, this is a challenge on the international scale.

How should individuals protect their privacy?

Everyone should be very careful regarding the online disclosure of their personal data. In particular, incentives such as special discounts in return for the disclosure of personal information should be treated with caution.

Which tasks do you think the BSI will face in future?

The BSI enjoys a great reputation in matters of IT security in Germany and beyond. Its recommendations and warnings are of interest both to the general public and to industry professionals. We need to maintain and build on this reputation. This will mean careful management of our priorities, as the BSI’s limited resources mean it can tackle only the most pressing challenges in the world of IT.

SSL-Security for Android

Problems revealed

SSL encryption can pose problems for users, administrators and developers – as studies by the Fraunhofer Institute for Communication, Information Processing and Ergonomics show.

With a market share of over 80%, Android is the most widely used operating system for smartphones. The majority of all Android apps have legitimate reasons for exchanging data with the internet. In so doing, however, these apps become responsible for the protection of sensitive user data. The Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are encryption protocols introduced to protect network communications from eavesdropping and tampering. Researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) have now discovered numerous and serious problems in their practical implementation, experienced by developers and administrators as well as users.

Developers often find the programming of SSL libraries too challenging. A study of 13 500 Android apps found numerous apps with insecure SSL connections. Almost 20% of the examined apps using SSL were found to contain potentially insecure code, including those offered by providers such as American Express, Diners Club, Paypal, Facebook, Twitter, Microsoft Live ID, remote servers, bank accounts and mail accounts. The total number of installations for this sample alone had, according to Google Play Markets, reached between 39.5 and 185 million. A small number of developers are therefore putting millions of users at risk.

Administrators, too, are experiencing problems with SSL: for a second study, researchers at the FKIE contacted some 8000 administrators of web pages with incomplete or faulty SSL certification. The 755 respondents cited the complexity of configuration, the high cost factor and a lack of confidence in the Certification Authorities as the reasons for the errors in their SSL certification.

Another study investigated whether users can differentiate between a regular http connection and an https connection on Android and whether they notice an SSL warning. The majority of participants (among them 57.6% of non-experts and 52.3% of IT experts) claimed never to have seen an Android certificate warning. 24.0% of participants read the warning only partially and 4.5% did not read it at all. As to the security of the SSL connection, the results showed that 47.5% of non-expert respondents believed they were using a secure connection, even though the survey was conducted via http. Moreover, even amongst participants with IT expertise, 34.7% claimed to be using a secure channel, although this was not the case. Only 58.9% of experts and 44.3% of non-experts correctly identified the connection as safe or unsafe respectively.

Overall, the entire SSL ecosystem needs to be reconsidered with a view to making it more transparent and people-friendly. Researchers in the Usable Security & Privacy Group at the FKIE have already developed initial proposals for solutions, but there is still much work to be done in developing people-friendly security solutions and establishing them on the market. □

Prof. Dr Matthew Smith,
Fraunhofer Institute for Communication, Information Processing and Ergonomics
Prof. Dr Peter Martini,
Director of the Fraunhofer Institute for Communication, Information Processing and Ergonomics

Alliance for Cyber Security

United against attacks

Since it was founded by the BSI and BITKOM in 2012, the "Alliance for Cyber Security" has steadily increased in importance.

By now the Alliance has over 1000 participants and counting. Further institutions, associations and companies – from DAX-companies to SMEs – are joining every day. The alliance provides companies with a comprehensive range of information including recommendations, analyses and monthly assessments of their cyber security situation as well as numerous opportunities to share experiences. Companies can inform the Alliance's registration office about any IT security incidents directly and anonymously. □

INTERVIEW

"WE MUST HEIGHTEN AWARENESS"

How do you assess the risk of cyber attacks on industry?

Digital interconnection is a competition factor for German industry. Whilst this brings many opportunities, there are also risks involved. The dismantling of boundaries between corporations, the closer integration of suppliers and service providers as well as the frequent use of wireless communications all facilitate attacks on companies' IT systems. The potential for damage caused by cyber attacks is enormous. Many thousands of cross-border attacks on German IT infrastructures are carried out independently by criminal organisations and foreign intelligence services. The theft, manipulation or illicit surveillance of data and sabotage of technical systems often go undetected. The losses caused by cyber attacks have far-reaching consequences for companies: security experts estimate an annual damage in the double-digit billions. The real figure could be much higher.

What trends are you observing amongst attackers?

Besides the increasing number of cyber attacks, it is especially the way in which companies find themselves under attack that changes, as does the speed with which new viruses are created and distributed: new malware is developed every two seconds. Attacks are now targeted and directed at companies, governments or the military. Medium-sized companies are particularly affected.

Deborah Klein,
IT Security Specialist, Department "Safety and Natural Resources", Federation of German Industries, BDI

INTERVIEW

Where do you see the greatest need for action?

Medium-sized enterprises in particular need to be further sensitised to the issue of cyber security. Progress must also be made regarding the cyber security of technical and human resources of small and medium-sized enterprises (SMEs).

What course of action do you recommend?

Though there is no absolute guarantee for security, we can make life as hard as possible for attackers. With preventive measures and not least with reliable IT security technologies, companies can achieve a high level of security. However, only those who are informed about the potential dangers can implement appropriate countermeasures. This includes drawing companies' attention to possible cyber security hazards, notifying them about imminent threats and taking adequate precautionary measures. Voluntary initiatives such as the "Alliance for Cyber Security" make an important contribution.

What is the significance of the "Alliance for Cyber Security" in this context?

*Cyber-security is a task for the whole of society. The long-term strengthening of the IT security infrastructure must be a common goal for industry, politics and society. The "Alliance for Cyber Security" is a very good example of how cooperation like this can be successful. Government and industry work hand in hand to prevent cyber attacks. In concrete cases, a wide network can then be activated quickly and efficiently. As the study "IT security in Germany, Recommendations for targeted implementation of the IT-Security Law" (***www.bdi.eu/Sicherheit.htm***) shows, companies want the BSI to provide an active information policy in the form of practical experience in the prevention of and defence against IT security attacks. The BDI and its member associations BDLI, BDSV, BITKOM and ZVEI jointly commissioned KPMG with the study.*

What is the BDI's view of the Alliance?

The BDI has supported the work of the Alliance from the beginning. The BDI agrees with the Alliance's goal of promoting cooperation and the exchange of information between companies and authorities on a voluntary basis. As a multiplier, the BDI would like to draw the attention of companies and affiliates to the work of the Alliance. Currently, the BDI is supporting the "cyber security survey of the Alliance". On the Alliance's Advisory Board, the BDI represents the interests of German industry at a high level. The BDI is also convinced that the principle of voluntary participation is the right approach.

www.bdi.eu/IT-und-Cybersicherheit.htm

Allianz für Cyber-Sicherheit

The Alliance in numbers

1 004 participating companies (October 2014)

1 605 participating employees (October 2014)

30 Events about the issue of cyber security in the first half of 2014

161 322 Visitors to the website www.allianz-fuer-cybersicherheit.de in the first half of 2014

The minimum latency and multi-point encryption of the network encryptor by manufacturers Rohde & Schwarz are based on suggestions by Alliance participants.

"THE RIGHT IDEA AT THE RIGHT TIME"

What concrete advantage do you gain from the Alliance for Cyber Security?

For us, the Alliance represents an attractive opportunity not only to exchange information with the security agencies and IT security research institutions, but also increasingly to interact with users in the business sector concerning their concrete needs for technical solutions in daily operations. Exchanging experiences with Alliance participants makes it easier for us to tailor encryption solutions so that they do not noticeably affect the operational network and production operation of the user and yet significantly increase the level of protection. During the Alliance for cyber security's participant days, we witnessed inspiring speeches as well as good opportunities to exchange ideas and experiences.

Peter Rost,
Rohde & Schwarz SIT,
long-term supplier of encryption techniques for use by public authorities

Were you able to make a contribution of your own?

We have been supporting the initiative with the aim of making a contribution to improving cyber security among the participants of the Alliance since mid-2012. In autumn 2013, for instance, we created a "checklist for network security" as a partner contribution. On the same topic of safe and efficient connectivity between locations and graded security through the establishment of network zones, we also organised day seminars.

How do you rate the importance of the Alliance for Cyber Security?

The Alliance for Cyber Security has developed into an impressive success story in the past two years: a rapidly growing number of participants and, in particular, the expanding network of multipliers speak for themselves. The idea of creating a platform for the exchange of confidential, practical aspects of cyber security in Germany came at the right time. The Alliance for Cyber Security is an essential component in improving the level of IT protection in Germany. We are happy to be a partner in this Alliance and look forward to the next steps together.

INTERVIEW

Electronic identities

Tools for online use

De-Mail and identity cards with an online identification function are key components of the Federal Ministry of the Interior's e-government initiative. Implementing them is an important task for the BSI.

Electronic identities are the basis of our online activities, whether in e-government or e-commerce. Our task as a central service provider for information security in Germany is the development and provision of secure "eID technologies" (technologies establishing electronic identities) on the one hand and their evaluation and analysis in close cooperation with administrative bodies, businesses and research institutions on the other, to enable trustworthy, authentic and legally binding actions online and prevent identity theft. As the body responsible for the overall infrastructure of official documents, the BSI coordinates the correct implementation of all the requirements.

The law for the promotion of electronic government (e-government law), adopted on 25 July 2013, defines the legal basis and therefore the tools with which the state is taking significant steps towards digital administration. The e-government law contains substantial changes to administrative procedures. Besides the qualified electronic signature, it introduces two additional technical possibilities of replacing the written form with electronic communications: the use of the online ID function for identity cards (eID function) and De-Mail. As of 10 October 2013, De-Mail is recognised by the courts as a secure transmission path for electronic submissions to the court, in line with the law in support of e-Justice.

The implementation of these arrangements will have a significant effect on citizens: the increasing availability of digital services is making administration ever more citizen-oriented as administrative errands can increasingly be taken care of online. The increase in efficiency of internal administrative processes and the associated reduction in bureaucracy will provide a measurable cost-benefit improvement for both administration and citizens.

What does the e-government law regulate?

- Replacing the written form with the online ID function and De-Mail
- Electronic access to administration
- Electronic records management
- Electronic payment
- Design of data formats
- Accessibility for digital administrative services

Dr Astrid Schumacher,
Head of Section
"Secure eID-Applications"

1. Online ID Function

The new ID card's eID function enables the secure authentication of citizens, using the so-called two-factor authentication procedure to protect them against identity theft. To be able to use this function, citizens need a specific software application on their home computer. This can be either the centrally-provided ID app (the development of which is managed primarily by the BSI) or a market alternative. In return, providers of online services make the eID function part of their process to verify the identity of their electronic communications partner.

www.personalausweisportal.de

2. Trustworthy administration and replacement of the written form

To assist public administration in the design of e-government administrative services, the BSI started the development of a technical guideline (BSI-TG 03107 "Electronic Identities and trust services in e-government"), in 2013. Part 2 of the guideline describes how to use safe online forms in connection with an electronic identity card's online ID function. Part 1 of the guideline is a substantial contribution to secure identity management, as it examines various confidence levels and assessment criteria that put the authorities in a position of being able to offer secure online services in line with data protection requirements. These developments have influenced both the German IT Planning Council's eID strategy and the implementation of the EU Regulation on electronic identities and trust services. ›

De-Mail

De-Mail enables the binding and confidential delivery of electronic documents and messages. The De-Mail law, which entered into force on 3 May 2011, specifies that all providers of De-Mail are tested and certified according to the same criteria in a transparent process.

This ensures that De-Mail is provided with a uniform level of security across Germany. In contrast to conventional emails, De-Mails are sent via encrypted routes and the identity of both correspondents as well as the sending and receipt of De-Mails can be reliably traced and verified. In this way, processes that previously required paper correspondence can now be completed electronically.

Accredited De-Mail service providers

- 1&1 De-Mail Ltd.
- Mentana-Claimsoft Ltd.
- T-Systems International Ltd.
- Telecom Germany Ltd.

3. De-Mail

According to Section 2 of the e-government law, every Federal Agency is required, in addition to the eID function, to provide access for the transmission of electronic documents via De-Mail. Furthermore, in line with Section 3a (2) sentence 4 no. 2 of the administrative procedures law, the written form can also be replaced by a De-Mail if the relevant De-Mail account has been "securely" accessed, e.g. by using an identity card's eID function. As the competent authority, the BSI is in charge of accreditation for De-Mail service providers. The company 1&1 De-Mail GmbH, for example, received its BSI accreditation as a supplier of De-mail services at the CeBIT 2013 in Hannover. The preconditions for the accreditation included an ISO 27001 certificate on the basis of IT baseline protection for 1&1 De-Mail's information network, certification of compliance with the Technical Guidelines for De-Mail service and a BfDI Privacy Certificate.

Trustworthy, authentic and legally binding

4. Electronic records management and archiving

Another essential objective of the e-government law is for administrative cycles – from application to archiving – to be completed without media discontinuity. In recent years, the BSI has developed technical guidelines for the area of electronic records, which provide pragmatic guidance for administrative bodies and businesses by setting structured requirements for the compliance with due process.

In this context, the BSI's Technical Guideline 03138, the "ResiScan", was published in 2013 to replace scanning. The TG is meant to serve users in administration, the justice system and businesses as a good practice guide for scanning paper documents whilst ensuring information security and then dispensing with the paper original whilst retaining the greatest possible security of evidence. The BSI-Technical Guideline 03125, "Retention of evidence for cryptographically signed documents", was further developed in 2013. In it, the BSI offers guidance on how data and electronically signed documents can be stored securely over long periods of time – until the end of the retention period – while preserving their evidentiary value. The BSI has already issued the first few certificates of conformity to these guidelines. □

"IMPROVED SECURITY FOR CITIZENS"

Cornelia Rogall-Grothe,
State Secretary at the Federal Ministry of the Interior and Federal Commissioner for Information Technology

INTERVIEW

Cornelia Rogall-Grothe has been a lawyer at the Federal Ministry of the Interior (BMI) since 1977. In 2010, she was appointed both State Secretary at the BMI and Federal Commissioner for Information Technology. In the following interview, she discusses the BMI's e-government initiative.

Ms Rogall-Grothe, the Federal Ministry of the Interior launched its e-government initiative for De-Mail and the identity card in March 2012. What was the motivation for this initiative?

We are keen for De-Mail and the online ID function of identity cards and electronic residence permits to become widely used across Germany, as they transfer personal data via encrypted channels and deliver them exclusively to previously identified correspondents. Besides being an improvement of online security for citizens, these two state-regulated IT infrastructures enable the wholly electronic (and therefore user-friendly and effective) management of administrative tasks, which citizens can now easily take care of from a computer and administrative bodies can process without media discontinuity. Our e-government initiative was launched to bring these benefits to citizens and public administrations. Administrative authorities at all levels should be encouraged to develop new attractive applications of De-Mail and the eID function for citizens. At the same time, the knowledge acquired by supported authorities can be documented and made available to other authorities for their own projects.

The second support phase of the e-government initiative ended in July 2014. What results have been achieved?

A total of 53 agencies at the federal, state and local level were given advice and support for the implementation of 71 projects developing attractive eID and De-Mail applications. 14 eID applications supported by the initiative had been launched online by May 2014 and four authorities had opened a De-Mail access point. The remaining authorities continue to work on completing their projects. Around 60 results documents – such as architectural and technical concepts, analyses of potential and technical and economic feasibility studies – can now be found on www.personalausweisportal.de and www.de-mail.de. There will be more to come throughout the year. Within two years, we have therefore been able to establish new and attractive services at all levels of government for both infrastructures and compile a broad knowledge base of implementation issues, which is available for all interested authorities to use. We have laid a strong foundation for the establishment of De-Mail and the eID function in German e-government.

Encrypted healthcare data

Extensive encryption measures ensure that the patient data on electronic healthcare cards remain protected. But what are the technologies that make this possible?

The electronic healthcare card (EHC) is designed primarily to enable medical applications, such as testing the safety of pharmacotherapy. However, the storage of sensitive health-related data can cause worries and anxieties. The project “telematics infrastructure (TI) in German healthcare” and the “society for the application of telematics in the healthcare card mbH” (known as gematik) deal with the question of how to meet the legally required service guarantee in line with § 291b of the SGB V, which includes: “protecting the interests of the patients”; “ensuring the necessary level of safety in the telematics infrastructure (TI)”; and “ensuring compliance with the provisions on the protection of personal data”.

The two-key principle

The two-key principle ensures that access to medical data requires the use of both the relevant EHC and a valid healthcare professional card (HPC). Only when the EHC has ascertained the presence of a valid HPC through successful Card-2-Card authentication in a heightened security procedure (i.e. after PIN entry) and the EHC holder himself has also entered his PIN, is access to the medical data or the use of the private key material on the electronic health card granted (see illustration on page 28).

Access to emergency medical data in the event of an actual emergency is an exception to the PIN requirement and use of this feature is voluntary. For obvious reasons, the active collaboration of the EHC holder cannot be guaranteed in an emergency. However, without the patient’s EHC PIN, access to emergency medical data is limited to certain types of health professional cards (HPC). “Bit 18” on the flag list of the healthcare professional card’s CV-certificate is required – which is activated only for doctors, their medical staff and paramedics. The technical implementation of access protection is carried out directly by the EHC’s operating system, thereby enforcing the patient’s rights. Moreover, the scope of access criteria to medical data is specified in the respective access rights regulation in §291a SGB V.

Decentralised storage

No medical applications in telematics (TI) currently operate a central storage service. All previously specified applications for the storage of personal medical data use only the EHC – that is if the data are not completely retained by the service providers, i.e. doctors, dentists, pharmacists, psychotherapists and their professional assistants. For future applications that may use an online storage service for professional medical data (such as the project “safety in pharmacotherapy”), the essential principle of individual patient data encryption via the EHC remains unchanged. Decryption of the data by the storage system’s operator therefore remains technically impossible. In this way, even medical data stored centrally online is available in plain text only locally.

The healthcare card must be safe.

Society for the application of telematics in the healthcare card mbH (gematik)

Closed network

The central network of the telematics infrastructure (TI) is a self-contained network. The only access options are via secure central access points, activated only in response to specific requirements of professional services and the society with the overall responsibility (gematik). Connection to the TI-platform is subject to the respective service passing gematik’s conformity assessment. Approved service provider institutions are then able to connect to the TI only via ›

How does the BSI support the security of patient data?

The restriction of access to medical data in the telematics infrastructure (TI) is generally enforced on the basis of technical procedures. The security of this method is mainly achieved through the continuous monitoring by the BSI of the development of subject-specific security concepts, by the BSI’s development of CC protection profiles and technical guidelines for the safety-relevant components of the telematics infrastructure (TI) and by the consistent use of appropriately certified products.

a BSI-certified connector and VPN access service.

Encoded transfer

The patient's medical data or other personal data are encrypted prior to any possible transmission away from the vicinity of the service provider. In addition, all communication connections within the telematics infrastructure (TI) are encrypted end-to-end. Within the connector's IPsec connection with the VPN access service, a TLS channel (at least TLS v1.1) is established leading to the appropriate specialist service provider. This means that even the operator of the telematics infrastructure (TI) network used for transmission, never comes into contact with the data of professional services in plain text. The figure illustrates the way in which the patient's EHC offers an encrypted channel to the card issuer's card management system, using the example of an update to the master data.

This is generally done via an existing IPsec connection from the connector to the central grid of the telematics infrastructure (TI). In addition, a TLS channel is constructed between card terminal and the connector, the connector and the intermediary and between the intermediary and the insurance's card management system (CMS). The communication between the CMS and the EHC takes place via secure messaging. The session keys for encryption or MAC-formation are derived individually using a "Shared Secret" known to the CMS and the EHC.

Avoiding profile compilation

The health insurance company is prevented from knowing the identity of the specific service provider through an intermediary, in order to prevent the compilation of a patient's movement profiles. This service is provided centrally by the telematics infrastructure (TI) and is therefore the responsibility of gematik.

Evaluated and certified

All cryptographic methods whose use is permitted in telematics infrastructure (TI) are listed in the technical guideline TR-03116-1 and are binding for gematik. The procedures and minimum key lengths listed here are internationally considered safe and include only public and standardised algorithms. In addition, the requirements for TR-03116-1 include time limits. The current version recognises the effectiveness of the specified cryptography until 2020. Those components of the TI-platform subject to the highest safety requirements (e.g. the chip and pin card, the card terminal or connector) must also be approved and certified according to the Common Criteria (CC), specifying that they have implemented the necessary cryptography correctly as well as meeting the safety requirements and underlying protection profiles. Manufacturers instruct BSI-accredited testing centres to evaluate their devices, which are then certified by the BSI. Both the BSI certification and the technical assessment by gematik are prerequisite for approval of the components.

Operational safety

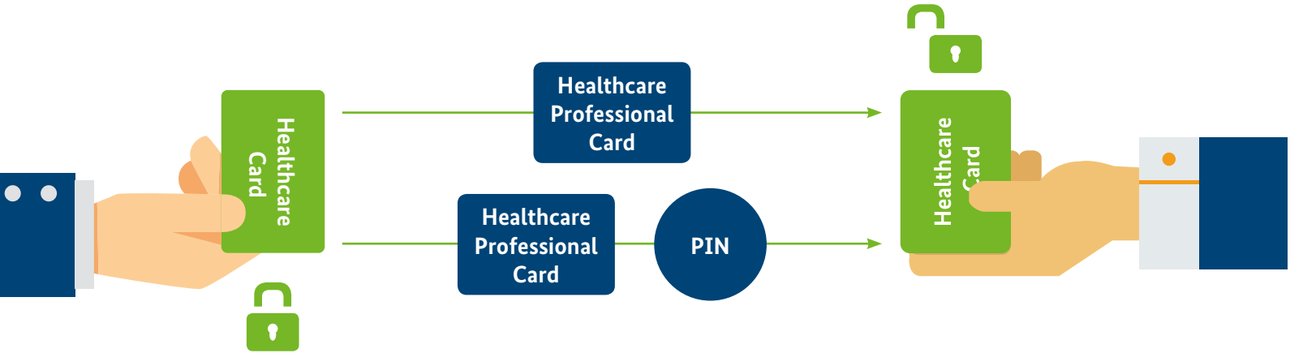
The construction and operation of an Information Security Management Systems (ISMS) according to ISO 27001, with specific characteristics for telematic infrastructure (TI), is mandatory for all operators of the central services of the TI and must be submitted for approval by independent security assessments every three years. The technical and organisational implementation of the requirements of Annex A of the ISO 27001 must, where the individual security requirements do not require higher quality measures, be carried out at least at the level of the corresponding basic protection requirements. In addition, all operators of the telematics infrastructure's central services are registered in gematik's coordinating information security and data protection management system.

The gematik society, because of its position of overall operational responsibility for the telematics infrastructure (TI), is classified as critical infrastructure in Germany and is a participant in the KRITIS Implementation Plan. In this way, gematik is able to maintain its high level of operational security. □

The gematik society, because of its position of overall operational responsibility for the telematics infrastructure (TI), is classified as critical infrastructure in Germany and is a participant in the KRITIS Implementation Plan.

Holm Diening,
Society for the application of telematics in the healthcare card mbH (gematik)

The two-key principle



Electronic payments – how safe are they?

Terms such as e-money, cyber-wallets and contactless payment are the clinking coins of the future. ePayBL is the platform for internet payments made by administrative bodies. What's it all about?

Although some citizens and companies still believe that the good old bank transfer or payment at the till are the only ways to pay fees and cost notices, the future of payment systems has already arrived in public agencies. With ePayBL, citizens can make electronic payments to administrative bodies, from anywhere and at their own convenience. Together with the states of Bavaria, Baden-Württemberg, North Rhine-Westphalia, Rhineland-Palatinate, Saarland and Saxony, the Center for Information Processing and Information Technology (ZIVIT) has been developing the payment platform ePayBL since 2002.

External financial service providers process the payments. The core component of ePayBL links the interfaces of financial services with the different specialised procedures and budgetary systems in the federal and state authorities.

Since 2006, the ZIVIT has operated the core component of the payment platform (which has now arrived at version 2.1) from its computing centre in Bonn. ePayBL enables the fully electronic administration of processes from electronic tolling and reporting, all the way to the processing and recording of the payment in the relevant authority's financial system, as required by Section 4 of the e-government law since 2013. The BSI and the ZIVIT are therefore taking a proactive approach to examining the information security of the platform and strengthening its development.

ePayBL is a web service that derives some of its functions from external bodies. As a first step, the ZIVIT and the BSI are closely examining the application of security policies and recommendations during the development of the web service. This concerns, for example, the exact definition of the access rights available to the developers of the software, in order to prevent the introduction of harmful functions. They are also considering the correct application of the elements in a programming language to be considered, e.g. checking externally supplied strings for faulty or harmful instructions.

Examine and develop

Given the importance of the platform for the public agencies using it, software tests should be extensive and pre-emptive rather than reactive. The overall architecture of ePayBL, including its numerous interfaces with external specialised procedures and users from federal and state governments, is subject to testing during its development. The BSI is involved in this cooperation as a consultant, due to its expertise in recommendations, requirements and guidelines for the development of secure web applications, IT baseline protection and its extensive knowledge of certification according to the Common Criteria. In the medium term, the BSI and ZIVIT will evaluate the ePayBL platform in operation. The range of services offered by the BSI in this context includes everything from testing for vulnerabilities in the IT systems, applications and the operating organisation to a certification for IT baseline protection. Security of payment data transmitted via insecure networks, the strength of the encryption process and the organisation in the distribution of encryption material constitute a wide field for testing.

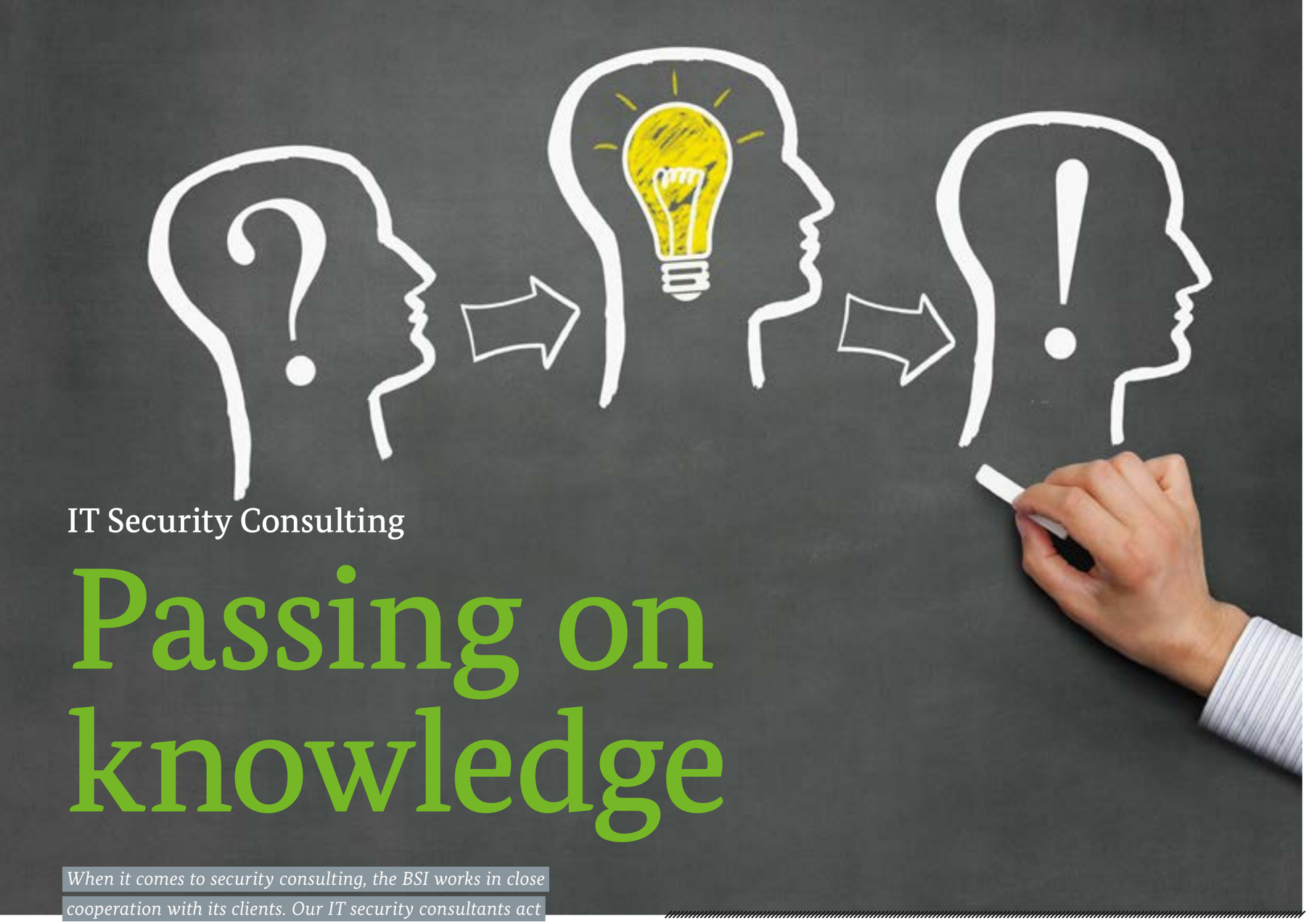
Electronic wallets are not e-mail accounts.

Electronic payment is deeply integrated in administrative processes.

Security managers must therefore pay close attention to all parts of the system.

The aim of the cooperation between the BSI and the ZIVIT is not only the examination of information security, but also to set a positive example for an excellent level of security whilst maintaining the usability of a platform. □

Dietmar Bremser,
Specialist, Section "Minimum Standards and Product Security"



IT Security Consulting

Passing on knowledge

When it comes to security consulting, the BSI works in close cooperation with its clients. Our IT security consultants act as the point of contact.

BSI's security consulting department is our designated point of contact (PoC) for the customer. Requests received by the BSI are centrally managed by our authority coordinators in that department. The aim of this centralised method of organisation is to optimise communication between our clients and the services of the BSI. In this way, requests for advice and support are answered either independently or with the involvement of the experts in the relevant units. In some cases, technical support is provided through the BSI's participation in projects or working groups. The consultation can also take the form of direct accompanying support or be performed on an individual basis to provide specific security solutions to technical problems.

The PDCA Model

Information security
... plan
... do
... check
... act

Günther Ennen,
Head of Section
"Security Consulting
for Public Authorities"

Further training enhances competence

When cooperating with the authorities, the company's "IT security officer" becomes the PoC on behalf of the client. This bilateral PoC structure guarantees smooth cooperation. In collaboration with the Federal Academy of Public Administration (BAköV), the BSI offers a training course for qualification as a certified "IT security officer". Our security consulting department is responsible for the content and structure of the course, supports the future IT security officers during training, evaluates and approves course projects and is represented on the board of examiners. The course includes detailed insight into the daily work of IT security teams and the responsibilities and competencies of an IT security manager.

For cooperation with the BSI to be successful, the customer must have an up-to-date Information Security Management System (ISMS). With this in place, the roles, skills and responsibilities of each actor are clearly regulated, arrangements are easily made, recommendations for security measures effectively implemented and advice and support are well received.

If the ISMS then follows the well-established PDCA model (Plan-Do-Check-Act), it will consistently comply with the thought process required in the face of new information security risks: continuous updating, adaptation and responsiveness.

Consulting target groups

Federal agencies constitute the primary target group of our security consulting service. Furthermore, we advise customers at federal, state and municipal level, as well as manufacturers, distributors and users on issues relating to information security. We also strengthen IT security in Germany through advisory (and lead) participation in the pertinent committees and by co-developing studies.

Companies can access the comprehensive database of information and solutions offered by the BSI, which is freely available on our website. A detailed individual consultation is carried out only in exceptional cases, to avoid any distortion of competition. Special regulations apply to companies in critical infrastructure, i.e. institutions concerned with public administration (tasks of particular public or political interest or further tasks in the "general interest" of the state).

In our experience, effective communication between the client PoC (the client authority's IT security officers) and the BSI's security consulting department optmisises workflows and ensures quality and efficiency. Information about services and IT security products is easily accessible via the section "Security Consulting" on the BSI's homepage. Information pertaining to selected target groups is archived in separate, access protected areas. IT security officers and confidentiality officers have access to these areas. □

Case by case

The BSI is involved in national and international efforts for greater standardisation, acting in an area of tension between legal requirements and standards.

In the field of IT, standards define quality requirements for products and are thereby decisive in the determination of their IT security properties: reason enough for the BSI be widely engaged in national and international standardisation efforts. In some cases, the BSI develops complete sets of technical specifications. In other cases, it guides, observes and comments on standardisation processes. When the BSI is legally required to provide the specification of technical standards, these are developed under active participation from the respective users, relevant standardisation bodies, manufacturers or authorities. The development of these standard security requirements for IT products is in many cases carried out on the basis of internationally recognised IT security criteria (Common Criteria, CC) and (where requirements for IT security management are concerned) under application of the international standard ISO 27001.

Protection profiles and technical guidelines

The BSI has developed high safety standards and functional requirements for the interoperability of communication units in smart metering systems with integrated security modules (the “smart meter gateway”), in the form of two protection profiles (PP) and a set of technical guidelines. The technical guidelines also define the system architecture, the public-key infrastructure and the requirements for safe technical operation of the smart metering system to be employed. Due to their special legal anchoring in the Energy Industry Act and related ordinances, the technical specifications for smart metering systems and their safe operation are binding for all market actors in Germany. The BSI is conducting further legally prescribed standardisation projects in the fields of regulatory documents, long-term archiving, security of satellites (in line with SatDSiG) and the protection of telematic infrastructure (TI) in healthcare. Certification allows the manufacturer to demonstrate compliance with the requirements of the relevant standards to third parties. In many cases, there is no legal basis for the BSI to develop legally binding technical requirements or for specific standards to be met. In the unregulated sector, standards are primarily developed through cooperation between experts from different manufacturers themselves. This process can occur in very different forms and lead to great variation in the quality of results. The spectrum ranges from de facto standards within individual companies, to standards applied by industry consortia, to those developed by official bodies such as the DIN or ISO/ IEC.

In the currently little regulated field of security chips, Germany has several strong, internationally successful manufacturers. In this instance, the BSI acts in close cooperation with these manufacturers to develop appropriate standards. Germany also enjoys a strong market position regarding control equipment for mechanical and plant engineering – keyword “industry 4.0” – but IT security is not currently a decisive issue in that field. Most other ICT product areas, such as network equipment, mobile devices, databases, operating systems, etc., are mainly dominated by American or, increasingly, Asian manufacturers. Options for German design and setting of standards are limited in this field. The findings and influence gained through participation in various committees will drastically increase in importance in the future. In the context of EU-level negotiations with the United States concerning TTIP (Transatlantic Trade and Investment Partnership), with Canada concerning the CETA (Comprehensive and Economic Trade Agreement) and with 23 other states concerning TISA (Trade in Services Agreement), the negotiating parties will also agree on standards that will ensure that market access for products and services in the field of IT. These deliver an important impetus for the development of standards set for IT security products at a national level.

No panacea

Standardisation is an important tool used by the BSI to promote IT security. It is not, however, a panacea for all security problems. While in the legally regulated areas the required IT security properties can be determined very directly, there are other market areas in which standardisation is difficult to achieve, for example due to a dominant provider wanting to prevent the market from opening. Since the conditions in which a standard is set vary greatly, each individual case must be assessed as to whether the BSI should become involved in the standardisation body and what form the involvement should take. In 2013, the BSI was engaged (either actively or as an observer) in about 50 different official standardisation bodies organised by DIN, DKE, CEN, CENELEC, ETSI, ISO/IEC and ITU-T. □

Tobias Mikolasch,
Head of Section
“Industrial Cooperation and Standardisation”

www.bsi.bund.de

Smart Metering

Intelligently measuring energy consumption

Germany is pioneering the use of secure smart metering systems in Europe. The sensitive consumer data generated constitutes a demanding task for the BSI.

Smart grids ensure that energy production and consumption are interlinked and balanced efficiently. Intelligent metering systems, so called “smart metering systems”, are key components. Smart metering systems are designed to ensure up-to-date consumption transparency and the secure transmission of data. They also control consumption through electronic equipment and production facilities, enabling a more efficient feed-in and management system within the distribution network. Since the processing of personal data is central to the construction and use of smart grids, ensuring the security and protection of that data is prerequisite for public acceptance of smart metering systems. In this area, the BSI develops protection profiles according to Common Criteria (CC – general criteria for the assessment of the safety of information technology) and technical guidelines that allow for an internationally comparable safety certification of corresponding devices.

Protection profiles and guidelines

In September 2010, the Federal Ministry of Economic Affairs commissioned the BSI to draft two protection profiles and a subsequent set of technical guidelines for the communication units in smart metering systems (the “Smart Meter Gateway”), in order to provide a single technical security standard for all market actors.

A protection profile systematically highlights threats to secure and privacy-friendly operation of the smart metering system and specifies the minimum requirements for appropriate security measures. On the basis of the protection profile, the products can then be tested. If it passes the set test, the product receives a certificate documenting its conformity with the protection objective. At the same time, the protection profile allows the manufacturer scope for innovation regarding the technical realisation of safety requirements. This enables a uniformly high standard of security whilst permitting variation in the execution of products and guarantees the continuing innovation as technical advances become available. Each protection profile’s security requirements are independent of technology and relate primarily to aspects motivated by data protection: the collection, processing and use of personal data and data security, regarding in particular confidentiality, integrity and authenticity. To ensure the interoperability of the different components in a smart metering system, purely functional requirements must also be met and the product design should take account of the security requirements in great detail. These additional aspects can be consulted in the technical guidelines (BSI TR-03109).

Security standards

Safety standards are effective only if they meet with broad acceptance among manufacturers and users. The BSI has therefore involved both groups in the creation and development of the two protection profiles and the technical guidelines from the very beginning. Associations in the fields of telecommunications, energy, information technology, housing and consumer protection were (in several rounds of consultation) extensively and significantly involved in the development of both documents. Overall, the BSI recorded around 1 200 comments regarding the protection profiles and more than 3 100 comments regarding the technical guidelines. These figures demonstrate the high level of interest the topic of smart metering systems is met with amongst experts and, increasingly, in politics.

Protection of privacy

During the development of the protection profile and technical guidelines, data protection requirements for the Smart Meter Gateway are considered alongside data security considerations. This is necessary in order to prevent the generation of detailed user profiles and the associated risk potential for scrutinising the end user’s lifestyle habits. To avoid this scenario, evaluation profiles in the smart meter gateway (SMGW) can be designed to allow the collection of only the necessary consumption data (relevant to billing), using a variety of decentralised, collective user profiles. This achieves both the stipulated data avoidance and the necessary data economy.

Statutory duty

Alongside extensive provisions for sector-specific data protection, the Energy Industry Act contains a ›

core provision (§ 21e), which requires the compulsory installation of a certified metering system in certain cases. In cases of buildings being newly connected to the power grid or having undergone extensive renovation, as well as in the case of customers with an annual consumption of more than 6 000 kilowatt hours, meter operators are legally obliged to install a certified metering system. Furthermore, according to the Renewable Energy Sources Act and the Cogeneration Act, operators of newly constructed energy systems with an installed capacity of more than 7 kilowatt must install certified metering systems. An amendment to the Renewable Energy Sources Act in 2014 ensured that, in future, the safety and interoperability standards already achieved in an amendment to the Energy Industry Act must also be applied to the cases described under § 34 and § 9 of the Renewable Energy Sources Act.

Intelligent energy management

The benefits of smart metering systems are especially evident for high-consumption groups (households and businesses), as their potential for energy saving and re-allocation is correspondingly greater than that of low-consumption groups. The Federal Ministry of Economic Affairs has created a cost-benefit analysis for further cases of mandatory installation of smart metering systems. In particular, smart metering shows great potential in the area of load- and feed-in-management, leading to a recommendation for the extension of compulsory installation to all cases of new renewable energy sources and cogeneration plants greater than 0.25 kilowatts. By controlling the distribution of loads and generators on smart metering systems, savings can be made in the course of network expansions in distribution networks. According to the cost-benefit analysis and prognosis, a roll-out of 11.9 million smart metering systems could be achieved by 2022.

BSI certification

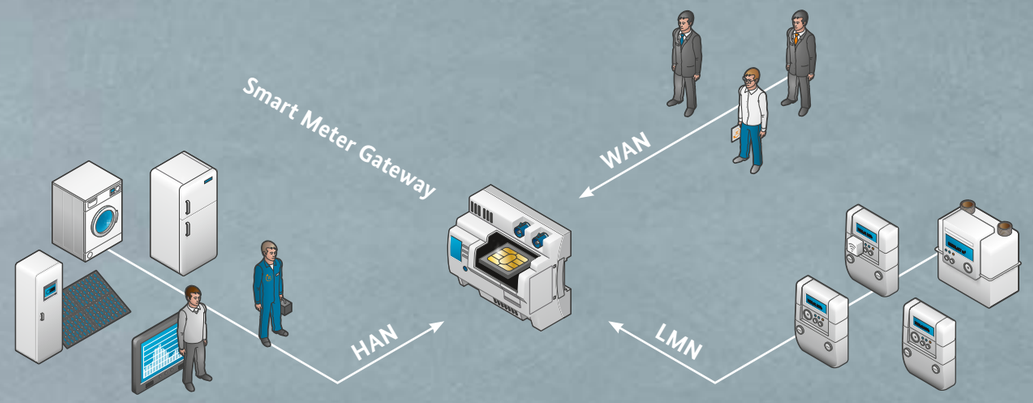
To ensure that a smart meter gateway meets the legal requirements of security and interoperability, the BSI must certify it regarding both its protection profile and its compliance with the technical guidelines. Furthermore, calibration regulations specify the need for a conformity assessment carried out by the Physikalisch- Technische Bundesanstalt (PTB). Care was taken to ensure that as many of the PTB's legal calibration requirements as possible were included in the BSI's documents during the development of the protection profiles and the technical guidelines, in order to avoid additional expense and the necessity for double-checks later on in the certification and accreditation process and in order to achieve synergies. The ministerial draft of the regulation for minimum technical requirements for the use of smart metering (the metering system regulation – MsysV), in line with § 21i of the Energy Industry Act, together with the two protection profiles and technical guideline 03109, passed the European notification process on 23 September 2013. According to EU Directive 98/34/EC, Member States are obliged to inform the European Commission about prospective national technical regulations, in order to identify and prevent trade barriers from developing. Adoption of the regulation through the national legislative process is planned for the second half of 2014, according to the coalition agreement between the CDU, CSU and SPD. ◻

Dennis Laupichler,
Specialist, Section
"Industrial Cooperation
and Standardisation"

www.bsi.bund.de/SmartMeter

Smart Meter Gateway

A smart metering system's lynchpin



A smart meter gateway (SMGW), with its integrated security module (SECMOD), forms the communication unit of a smart metering system – a central component that receives, stores and processes the data supplied by meters, making it ready for use by market actors.

The SMGW communicates with various components and market stakeholders for the purposes of both consumption data transmission and administration.

In the wide area network (WAN), the SMGW communicates with external market participants and particularly with the SMGW administrator. In the local metrological network (LMN), it communicates with the connected meters (electricity, gas, water, heat) of one or more end consumers. The meters communicate their measurements to the SMGW via the LMN.

In the end consumer's home area network (HAN), the SMGW communicates with controllable sources of energy consumption and energy production (e.g. intelligent home appliances, power-heat units or photovoltaic systems). Furthermore, the SMGW deposits data confidentially on the HAN, ready for use by the end consumer (or service technician). All communication flows are encrypted and secured with regard to their integrity, authenticity and confidentiality. In order to achieve this, the SMGW uses a so-called security module, which serves as a safe storage space for the required cryptographic key material. The security module also provides the core cryptographic routines for signature creation and verification, key generation, key negotiation and the generation of random numbers for the SMGW.

Cloud Computing

Trusting the cloud

Dr Patrick Grete,
Specialist, Section “Integrated Analysis of IT-Security Trends and Impacts”

Dr Clemens Doubrava,
Specialist, Section “Integrated Analysis of IT-Security Trends and Impacts”

Greater transparency is set to inspire new confidence in the security of cloud computing. The BSI has developed six building blocks for cloud risk management.

The deep uncertainty prevalent since Edward Snowden’s revelations has also affected the area of cloud computing. Renewed confidence will only be achieved through transparency. For secure cloud computing, the following three aspects arise:

1 Risk transparency

Risks to information security must be clearly identified and evaluated. It is the responsibility of the respective institution’s risk manager to decide whether or not to use a cloud service – a decision process in which the BSI can offer support. The strongly unified nature of processes, data and actors in cloud computing allows for a very systematic analysis of risks.

2 Open standards

The efficiency of cloud computing relies on its high degree of standardisation among services. This also benefits security and leads to a high level of trust, if the respective standards are transparent and can be openly discussed and evaluated. The same applies to the specific architecture of the cloud and to corresponding security certificates.

3 Clear separation

The transition to cloud computing is always accompanied by a distribution of the responsibility for information security – but the ultimate responsibility cannot be avoided. Accurate contractual regulation of this shared responsibility is therefore important in order to achieve clarity between users and operators.

Security and risk

As these points demonstrate, the BSI pursues a risk-based approach in cloud computing: information security risks cannot be entirely ruled out in distributed infrastructures such as cloud computing. They can, however, be reduced and must be actively controlled by risk management. On the issue of secure cloud computing, the BSI addresses several different target groups. Its website’s section on cloud computing (www.bsi.bund.de/cloud) has been redesigned and contains customised information for different target groups. Since the publication of its key issues paper “Minimum Security Requirements for Cloud Computing Providers”, the BSI has regularly published additional targeted articles in order to achieve the objectives listed above. These include six “Building Blocks for Cloud Computing” (one each for virtualisation, web applications, cloud management, web services, cloud storage and cloud use) for the Information Security Management System IT baseline protection. They describe the main threats and countermeasures relevant to each topic.

The six cloud building blocks can also be very helpful to non-users of IT baseline protection. The hazards listed in each one can be used by risk management to identify the relevant risks and the associated measures provided to form the basis of supplementary security concepts. Each building block contains a set of so-called Golden Rules, summarising its main requirements for the management level. They also constitute a checklist to be used in contract negotiations, so that any potential cloud service provider must provide information regarding the implementation of the relevant security requirements. These building blocks are therefore an important contribution to risk transparency. More transparency can also be achieved by a systematic method of risk assessment, which ensures the identification and application of appropriate measures in compliance with the relevant international standards and frameworks.

Security profile SaaS

The security profile for SaaS was published at the CeBIT 2014. For the application of customer relationship management (CRM), it describes all initially relevant actors, business processes and data, as well as the affected components of cloud architecture. That is where the following six hazards are relevant: simulation, manipulation, denial, loss of confidentiality, non-availability and escalation of rights. This interconnection results in all possible risks, as long as the stakeholder, data and business process model is complete. 13 of the most relevant risks are summarised in factsheets. These risks are countered with actions from different frameworks and standards: the BSI’s key issues paper, the ISO / IEC 27001, the CSA’s Cloud Control Matrix, the NIST 800-53 and FedRAMP. Specific security measures have also been formulated for the application of CRM. A cross-reference table matches security measures to hazards. It therefore becomes easy to identify which risks have been reduced and which residual risks remain. The security profile is a useful blueprint for any risk management strategy, as it systematically analyses risks, implements appropriate measures and gives an overview of residual risks. In this way, the provider can make informed decisions, which are also helpful to the user in contract negotiations. The BSI’s cloud security team continues to work on the above objectives for security in cloud computing and would welcome any suggestions for future discussions and ideas for new topics. The team can be contacted via **cloudsecurity@bsi.bund.de**. □

Secure cloud computing in the BSI

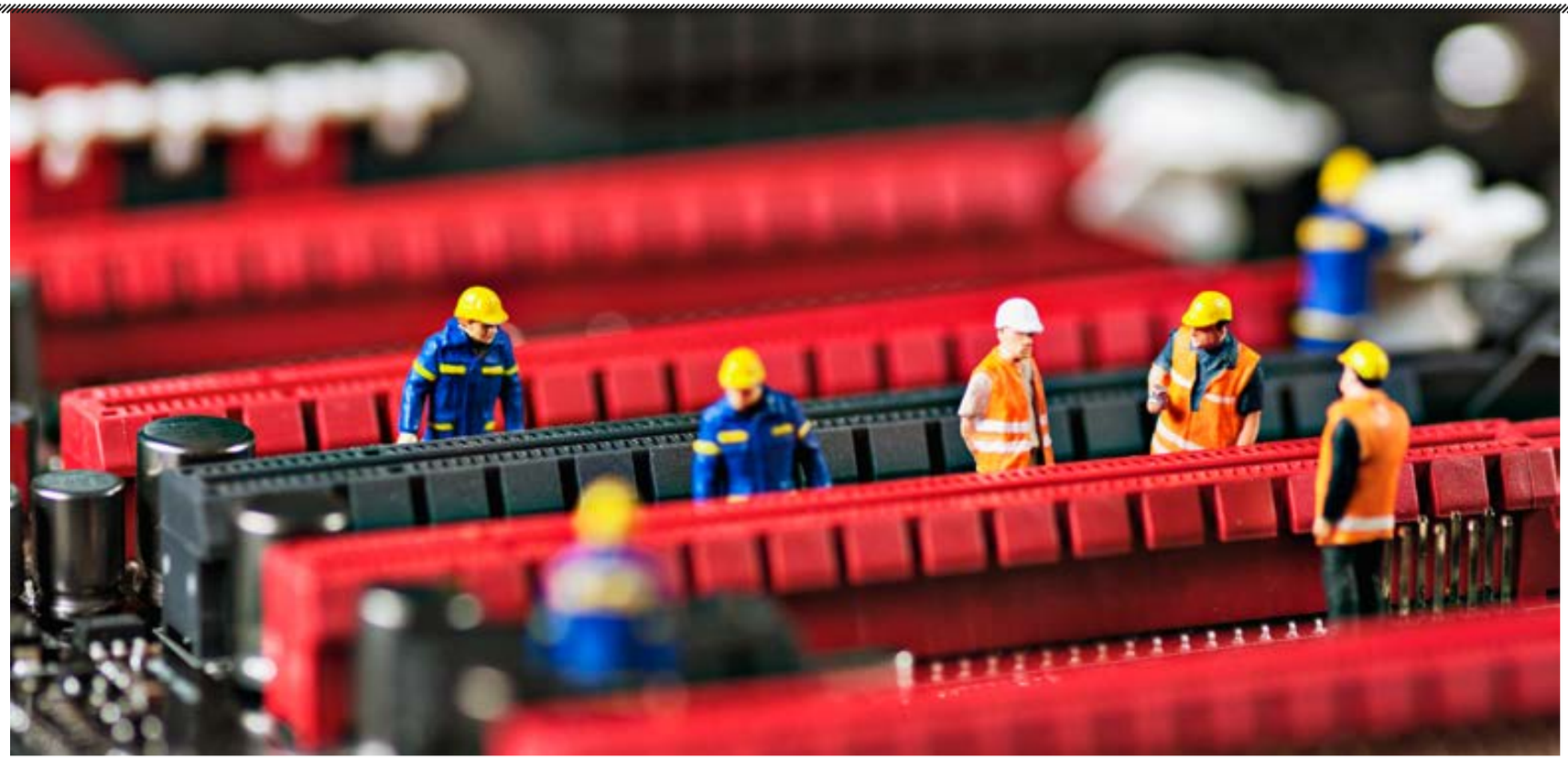
2014 Building Block for Cloud Use
Building Block for Updates to Storage Systems
Building Block for Web Services
Security profile SaaS
2013 Building Block for Cloud Management
2012 Building Block for Web Applications
2011 Building Block for Virtualisation, Key Issues Paper
“Safety Recommendations for Cloud Computing Providers”
2010 Preliminary version of the Key Issues Paper
2009 Building Block for Storage Systems
2006 First mention of the term Cloud Computing

www.bsi.bund.de/cloud

Industrial Control Systems

The right advice

With attacks on industrial facilities becoming commonplace, the BSI protects operators and manufacturers by giving them the advice they need.



Over the last few years, factory automation and process control infrastructures (categorised as Industrial Control Systems/ICS) have undergone some fundamental changes. From a security point of view, the main changes have been the massive increase in production networking, along with internal and external company networking. The use of commercial off-the-shelf components such as operating systems, databases and established conventional IT concepts and technologies has also become the norm. This means that modern cyber threats are also extremely critical for industrial control systems.

The number of security breaches affecting industrial control systems is increasing steadily and targeted attacks are becoming ever more common. Just a few years ago, attacks were largely confined to the theft of intellectual property, but today they are progressively targeting plant operations.

Three years ago, the BSI set up the Section for Cyber Security in Critical IT Systems, Applications and Architectures, a service dedicated to ICS security issues.

In recent years, this has led to the creation of a broad range of recommendations and aids designed to help manufacturers of industrial components, integrators and mechanical engineering firms as well as plant operators to achieve a sufficiently high level of protection for their products and production plants. As the issue of cyber security is still often neglected in the mechanical engineering and automation industries, it is important to find a straightforward approach that makes it easy for these sectors to get to grips with the topic and make steady progress in this respect.

Target group: Operators

For most operators, the **ICS Top 10 Threats and Countermeasures** provides an ideal introduction to the topic of ICS security. This report presents the most critical and frequently-exploited vulnerabilities that allow attackers to gain access to production systems. It gives advice on how to make initial assessments in specific cases and highlights appropriate countermeasures. The report also includes a short self check consisting of 30 questions designed to allow companies to make an initial assessment of their situation. These “Top 10 Threats and Countermeasures” are supplemented by a number of recommendations on specific issues such as insider threats or how to handle the discontinuation of Windows XP in a production environment.

The aim of these documents is to achieve some significant quick wins based on particular security scenarios and they provide businesses with a good introduction to ICS security, tailored to the individual situation. Raising awareness of ICS security is still quite a challenge however, so the report also provides a number of specific examples of security incidents that may be encountered in production and automation. Once operators have used these aids to begin tackling ICS security issues, other reports are available to help them make more progress with their cyber security, notably the BSI’s ICS Security Compendium. These essential guidelines help IT experts, IT security experts and production/engineering specialists to delve more deeply into the topic of ICS security. The main focus of the **ICS Security Compendium** is to provide a collection of best practices for operators with a view to increasing the security of new and existing facilities. They can be put into practice in a number of ways and are particularly suitable for plant automation and process control systems. ›

Start small, keep on growing, and think big.

BSI slogan for ICS

Certain topics – such as how to carry out security audits – are addressed in more detail in separate sections. The ICS Security Compendium is supplemented by **Light and Right Security (LARS)**, an ICS-specific security tool which helps operators to survey their systems and put in place the measures described in more detail in the ICS Security Compendium, so the that Compendium and LARS tool work together seamlessly. This software is available free of charge and has an open-source licence, so that (amongst other features) it can be adapted very easily.

Industrial control systems are not typically operated by IT specialists but by technicians and engineers. Both groups tend to be less IT-savvy and may not be fully aware of all the cyber security issues involved. In this circumstance, another useful aid provided by the BSI is the ICS Security Awareness Toolkit. The toolkit provides a brief guide to the key aspects of planning and implementing awareness-raising campaigns in businesses. This guide is supplemented by multi-media materials such as posters, text modules for companies to use on company intranets and in newsletters, videos, flyers and handouts.

The aim is to continue expanding this toolkit in collaboration with the industry. The Awareness Toolkit is especially useful to small and medium-sized companies (SMEs) that do not have the resources to run awareness campaigns, as they can use it to develop their own programmes.

Target group: manufacturers

BSI's slogan "Start small, keep on growing, and think big" is also perfect for manufacturers, mechanical engineering firms and integrators. The introduction includes advice on dealing with vulnerabilities and a check list of requirements for industrial network-compatible components. In the wake of Stuxnet, manufacturers have generally ramped up their efforts to make their products more secure, but many of them still have some catching up to do in this particular area. Manufacturers and integrators should aim to tackle security in a holistic way, viewing it as an integral component of the product lifecycle.

The challenge of Industry 4.0

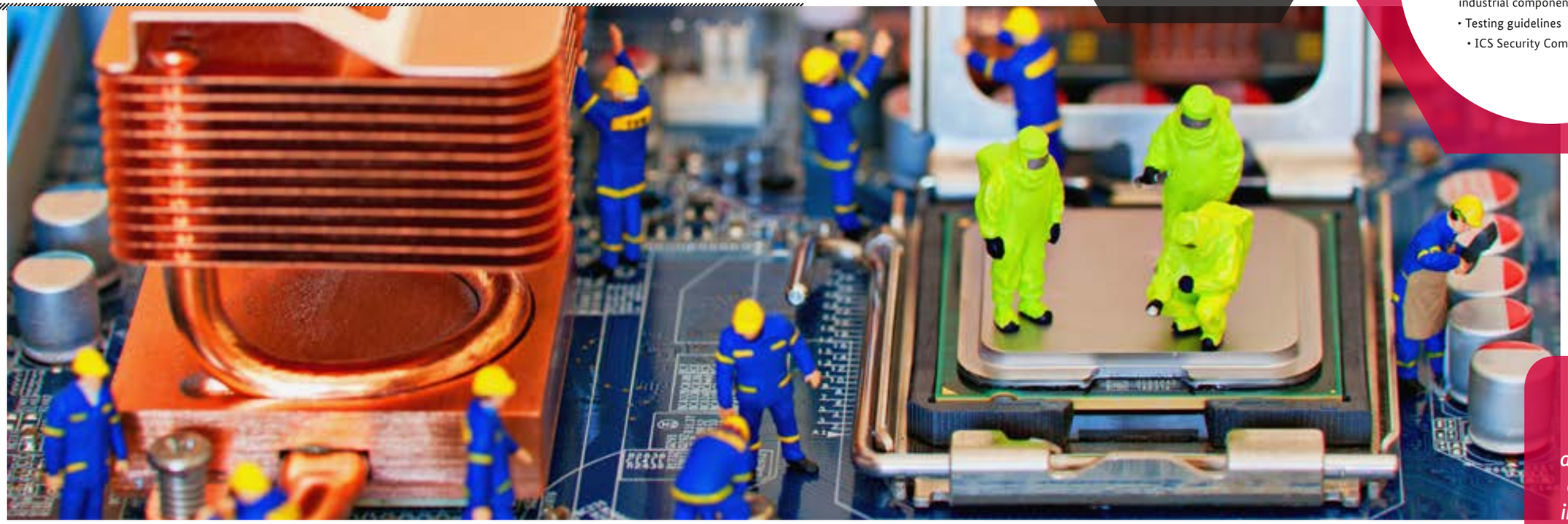
The advent of Industry 4.0 means that security has become a key factor in product marketing. The tried-and-tested solutions for existing production facilities have not kept pace with the massive increase in complexity that will accompany this major new development. There is a need for innovative approaches to roles and rights management, anchors of confidence and secure platforms. □

Operators

- Self check
- ICS TOP 10 Threats
- ICS Security Compendium
- ICS Security Awareness Toolkit
- Specific recommendations
- LARS

Manufacturers and integrators

- Dealing with vulnerabilities
- Demands on network-compatible industrial components
- Testing guidelines
- ICS Security Compendium



The number of security breaches affecting industrial control systems is increasing steadily.

Holger Junker,
Head of Section,
"Cyber Security in Critical IT Systems, Applications and Architectures"

Critical Infrastructures

The cross-sector collaboration between business and government on the UP KRITIS project (Critical Infrastructures Protection Implementation Plan) has provided a successful model for future initiatives. This joint project is constantly adapting to meet the needs of shifting threat scenarios.

Participation in UP KRITIS has grown significantly over recent years, and it is currently unable to accept new members. It was reorganised in 2013 in order to provide a two-stage membership model, which will allow it to continue with its positive collaboration and accept new members in future. The objectives of the joint project have also been realigned to take into account the new tasks and challenges it faces. UP KRITIS provides its member organisations with an opportunity to share knowledge and learn from each other. All members are linked to the BSI's warning and alert structures via their emergency contacts, so they are in direct touch with the BSI and the National IT Situation Centre. They receive situation reports and alerts from the BSI and make their own contributions to the joint status. This joint assessment of potential threats and risks is an essential element in preparing for IT incidents and (potential) IT crises. By sharing a common understanding of threats and implementing the appropriate crisis management structures, members can work together to deal with incidents – or even crises – swiftly and effectively. Regular exercises are carried out to check whether the agreed communication structures can be improved or maintained and whether the crisis management structures and processes are efficient and effective.

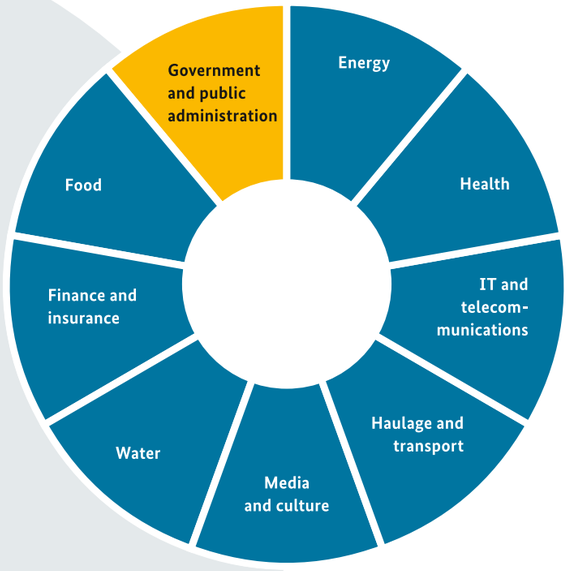
Incidents and shortfalls, for example in energy supply, can have a major impact on broad swathes of the population.

UP KRITIS

Nora Apel,
Specialist, Section "Critical Infrastructure Protection"

Critical infrastructures in Germany

Critical infrastructures are the lifelines of our society. They provide important and sometimes essential goods and services that are vital for the nation, i.e. for the economy, government and society. The German federal government's strategy on critical infrastructures defines them as "facilities and organisations of major importance to society whose failure or impairment would cause a sustained shortage of supplies, significant disruptions to public order or other dramatic consequences" (this document can be downloaded at **www.kritis.bund.de** under "Publications"). Critical infrastructures in Germany include installations and organisations in the energy sector, IT, telecommunications, haulage, transport, health, water, food, finance, insurance, government, public administration, media and culture.



Understanding threats

The BSI works with operators of critical infrastructures from different sectors in a series of industry working groups on IT/cyber security. These are designed to prevent incidents or breakdowns in IT and information infrastructures. Operators of critical infrastructures and BSI representatives regularly come together in these working groups to discuss cyber threats in particular industries. The aim is to come to a shared understanding of the IT/cyber threat situation and agree on how best to mitigate risks, identify incidents and, where necessary, deal swiftly with crises (IT-related or otherwise). Over recent years, the issue of cyber security has gained in significance as the production and supply processes of critical infrastructures – and therefore supplies to the population – increasingly depend on the reliability of IT functions. This increases the risk of IT-related incidents or shortfalls in (critical) services. UP KRITIS is open to any organisation that has its headquarters in Germany and operates critical infrastructures in Germany. Membership is also available to national trade and industry associations from the critical infrastructure sectors and to the public authorities responsible for these areas. □

www.upkritis.de
www.kritis.bund.de

IT security in the political sphere

Politicians are increasingly turning their attention to the issue of IT security. The BSI is on hand to offer expert advice.

In the political sphere, awareness of IT security has grown steadily over recent years in tandem with society's increasing digitisation. 2013 was an eventful year in this respect, providing many initiatives which served to heighten this awareness. Early 2013 saw the presentation of the draft IT Security Law. One month later, the German Bundestag's inquiry on "The Internet and digital society" presented its findings to parliament. In the summer of 2013, in the wake of the Snowden revelations, the German government created an eight-point programme to protect privacy, which once again turned the political spotlight onto the issue of information security. This coincided with the run-up to the parliamentary elections in which many parties and political interest groups took a stance on issues relating to IT security.

The growing significance of IT security was also reflected at the end of November 2013 in the coalition agreement for the 18th legislative period. This agreement mentions digitisation as a key challenge and proposes a number of actions to promote IT security. The coalition agreement includes an announcement that the new legislative period will include a new IT Security Law and a commitment to increase "trust in the Internet infrastructure of Germany and Europe". The BSI is also explicitly mentioned in the sub-section on digital security and data protection, in which the coalition partners state they will "increase the powers of the Federal Office for Information Security (BSI) and the Cyber Defence Centre." The coalition agreement also addresses a number of BSI issues, including the "further development and distribution of chip card readers, cryptography, De-Mail and safe end-to-end encryption" and the introduction of "certification for cloud infrastructures and other sensitive systems and services". The work of the BSI has also been affected by the announcement of ›

the Digital Agenda 2014–2017, a cross-departmental initiative which will set out the key points of the federal government's digital policy. As an independent and objective point of contact for questions on IT security in today's information society, the BSI provides politicians with expert advice on technical issues relating to information security and digitisation when they are drawing up and implementing policy measures on IT security. In 2013, the BSI was once again involved in advising government committees such as the Committee on Internal Affairs, the Parliamentary Control Panel (PKGr) and the ICT Commission of the Council of Elders of the German Bundestag. It also received numerous speaking invitations from political stakeholders. The issue of transnational IT security has also increased in significance, meaning that the BSI's expertise is also in demand at European and international level.

The growing political importance of IT security affects the BSI's activities, as technical questions can no longer be viewed as being triggered by the expectations and demands of political players. Now these questions tend to emanate from countless interactions between developments in the political sphere and the tasks of the BSI as an expert body. The BSI has to deal with these by ensuring that chief officers are regularly prepared for hearings in front of government committees or for dialogues with political stakeholders.

Oliver Klein,
Specialist, Section
"Integrated Analysis of IT Security Trends and Impacts"

These developments will continue in 2014, as demonstrated by the ongoing work on the Digital Agenda 2014–2017. The BSI's expertise will also be in demand by another parliamentary committee, the Digital Agenda Committee, which began its work in 2014. It has been set up in the wake of the final report by the "Internet and Digital Society" inquiry, published in early 2013, which called for the establishment of a permanent parliamentary committee on Internet policy. A number of new working groups and initiatives have also been set up to tackle information security in response to the ongoing digitisation of business, public administration and society as a whole. The pace of development and the political relevance of digitisation will continue to grow, so in future the BSI will also accompany these developments at political level and act as a trusted, expert adviser to political stakeholders on information security issues. ◻

Political voices

"Citizens cannot take sole responsibility for their security – and equally, governments cannot be solely responsible for the Internet security of their citizens."

Thomas de Maizière (CDU), Federal Minister of the Interior, Alfred Herrhausen Society conference, September 2014

"IT security has become an essential prerequisite for the protection of civil liberties."

From the coalition agreement between the CDU, CSU and SPD, 18th legislative period

The IT Security Law

For society as a whole

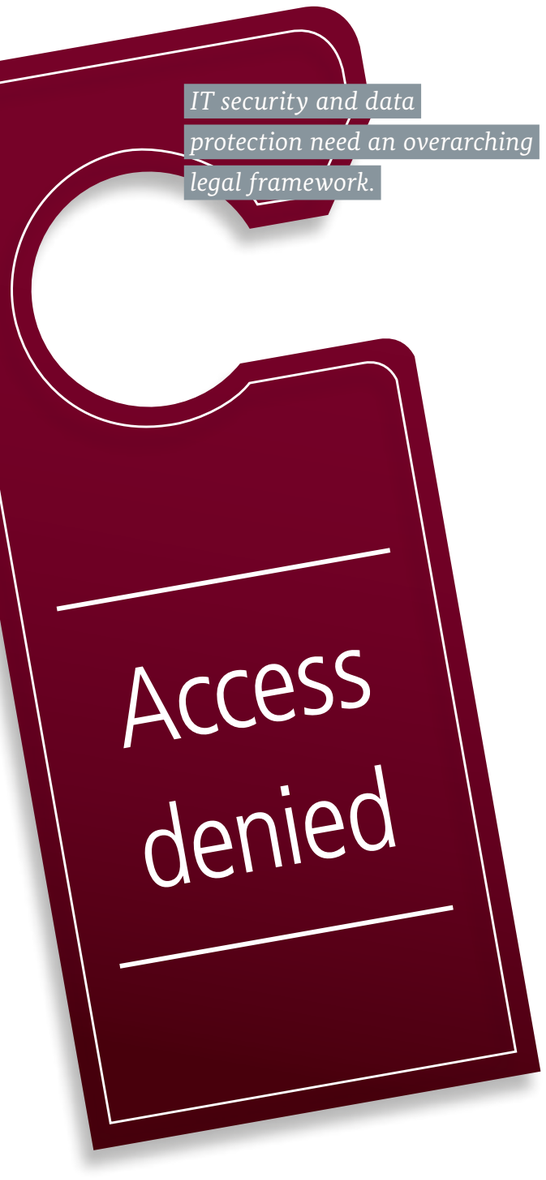
Public and politicians alike are becoming increasingly aware of the issue of IT security. The new IT Security Law is designed to protect businesses and private individuals.

We are bombarded by media reports about attacks on IT systems or vulnerabilities in popular programs and devices. So it is hardly surprising that users are wondering whether and how they can continue to safely use modern technology. In their coalition agreement, the ruling parties have therefore identified IT security as a key focus for the current legislative period.

The Minister of the Interior is also addressing this issue. Along with making organisational changes to tackle the problem of cyber security within the BMI, Dr Thomas de Maizière has made several public statements in favour of strengthening the BSI. Shortly after taking office, he also declared that he would continue the work that was begun in the last legislative period on drafting an IT Security Law. Whatever laws are finally passed by the Bundestag, one thing is clear: robust IT systems for operators of critical infrastructures are an essential foundation for supplying the public with vital goods and services. The Stuxnet worm impressively demonstrated to the wider public that industrial control systems can be extremely vulnerable. So the new law will oblige operators of critical infrastructures to protect their IT systems in such a way that cyber attacks cannot lead to supply shortages. It also seems likely that it will oblige them to disclose any major IT security incidents. On this basis, the BSI will be able to create a consolidated situation report, inform other operators about potential attacks and recommend more targeted protective measures. It is also clear that the advent of the IT Security Law means that the BSI will have to take on a new role. It will move from being the German government's information security provider to being an institution that serves society as a whole. This journey began with the last amendment to the BSI Act in 2009. Today, citizens, businesses and politicians all expect the BSI to provide them with support on IT security issues in a digital world that is becoming more complex every day. The BSI has reacted to this demand by expanding its services for citizens (such as BSI for Citizens) and for businesses (such as the Alliance for Cyber Security). Legislators have reacted to its changed role by drafting the IT Security Law. ◻

Steve Ritter,
Specialist, Section
"IT Security and Law"

Keeping it confidential



IT security and data protection need an overarching legal framework.

IT security is entering a new era. In the wake of the Snowden affair, revelations that millions of eBay accounts have been hacked and countless other minor scandals, the IT security and data protection industries are now grappling with the question of how public authorities, businesses and private individuals can maintain the confidentiality of their communications. How can we ensure that the intelligence services of any nation and criminals of any hue are not in a position to watch us, eavesdrop on our conversations and spy on us? And how can we protect our personal data? All these incidents have resulted in major doubts about information technology and IT security. Data protection is a hot topic. At a time when the world is more connected than ever before, we now find ourselves losing confidence in the technology that has brought us to this point and questioning the security that should be provided by data protection laws. It is an issue that affects every one of us: public authorities, businesses, private individuals, consumers and producers, young and old.

The first proposals to be put forward included the widespread use of encryption on the technical front and a treaty to ban this kind of espionage on the legal front. But is this enough? In technical terms, encrypting communications and stored data is certainly a way of shielding them from curious eyes. A "No Spy" treaty would probably help. But is this enough to provide the required level of protection against spying by foreign governments, criminals and companies? And do these measures provide the protection that is needed in light of ongoing technical advancements? The transition from paper to the digital world is unstoppable, so it is important to create a broader foundation for IT security and data protection. For Germany and Europe, security and data protection technologies are increasingly creating a locational advantage that is appreciated at home and abroad. Technology is becoming a decisive factor and provides the link between application and user. So it must take into account the requirements of data protection laws and IT specifications.

Protecting the public

A society which is increasingly reliant on electronic processes also creates new critical infrastructures that are not only of interest to intelligence services but also involve other actors. Protecting these critical infrastructures is a challenge that governments have to face if they are to protect their citizens and their freedoms. Without this protection, no free society can continue to function in the long term. So IT security and data protection are two sides of the same – very valuable – coin.

In light of this, it is vital to go beyond individual measures and integrate IT security and data protection laws into an overall concept that is viable for the future. The German government is planning to use its IT Security Law to improve the security of all critical infrastructures in the economy, increase transparency with regard to potential risks and incidents and at the same time use the knowledge and expertise of international networks with regard to threats in order to increase security as a whole. Data protection will also be given greater emphasis and made a key focus.

The NSA scandal has revealed the vulnerability of digital society and the urgent need for new legislation. IT security and data protection are prerequisites for upholding civil liberties. I whole-heartedly support the government's initiative because, at the end of the day, it will also benefit data protection. The often selective introduction of encryption and new treaties will not be enough to protect us in the future. An overarching initiative is the only way to protect critical infrastructures. □

Andrea Voßhoff,
Federal Commissioner for Data Protection and Freedom of Information

The BSI and public relations

IT security affects us all

Newsletters, social media and websites are just some of the many channels used by the BSI to keep the public up to date.

Every day the BSI receives countless queries on IT security issues. The objective, independent and expert advice that it provides is much appreciated, showing that the BSI has become a go-to resource for many users. With practical assistance and useful tips, we work hard every day to help citizens be more aware of how to use information technology in a safe way.

Websites

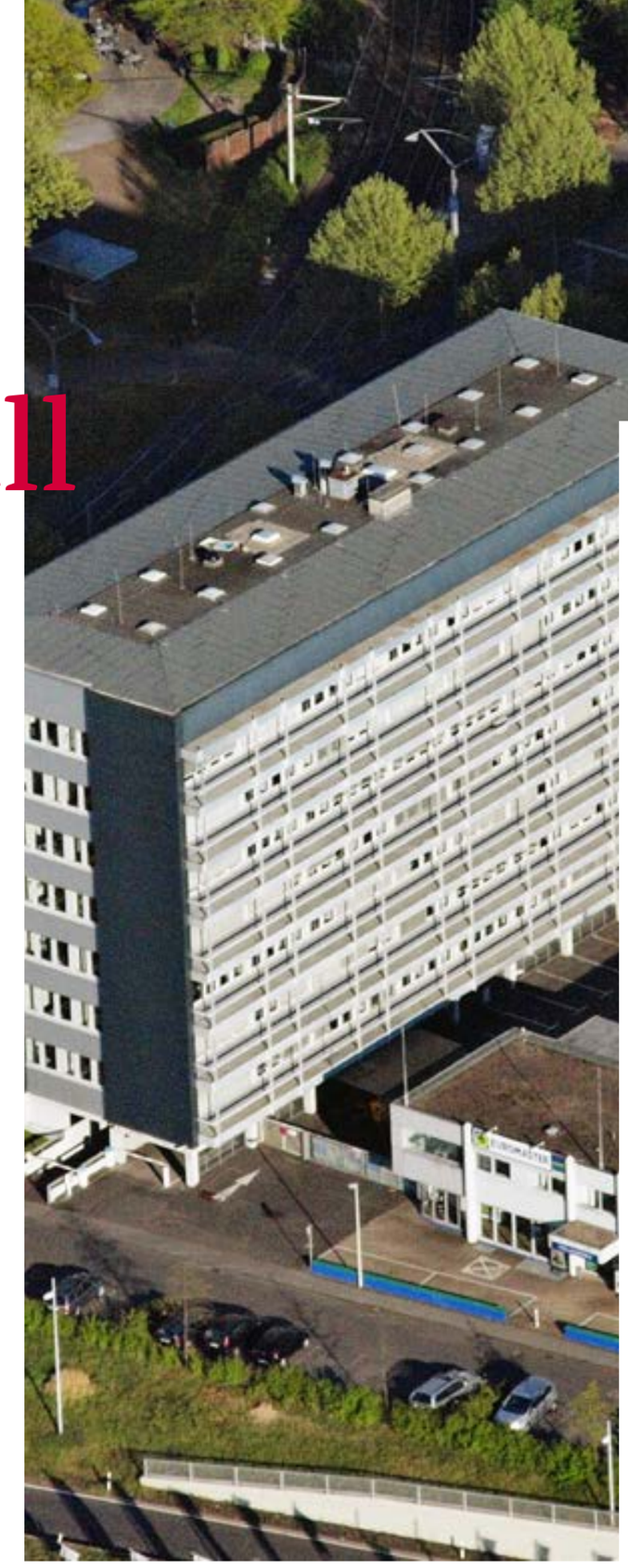
But people have to understand the assistance and advice provided before they can put it into practice. So the BSI provides specific information for different needs and target groups. The **www.BSI-fuer-buerger.de** website presents complex topics in clear, simple language. It provides practical tips and check lists so that users can learn how to improve IT security on their devices. For IT experts, the **www.bsi.bund.de** website covers a wide range of topics such as critical infrastructures, basic IT security and security consulting. This is where to find the latest press releases, studies or warnings about critical vulnerabilities.

Newsletter

The newsletter Safe • Informed from BSI Citizens CERT is available free of charge every 14 days. It provides fast, reliable information on viruses, worms and vulnerabilities in computer applications. Over 100 000 users have already subscribed to the newsletter at **www.buerger-cert.de**.

Facebook

The BSI Citizens portal has had a Facebook page since August 2013. From Monday to Friday, the editorial team makes daily posts at **www.facebook.com/ BSI.fuer.buerger**. They include regular features, security tips, multimedia materials and articles on IT security topics. Facebook fans and visitors can interact directly with the BSI by commenting or sending private messages. This page and its opportunities for interaction have proven to be a great success, demonstrated by the fact that it has attracted more than 21 000 "Likes" in its first year.



Information for citizens

Newsletter "Safe • Informed"

26 (2013)

13 (by July 2014)

Extra issues "Safe • Informed"

5 (2013)

6 (by July 2014)

Technical alerts

109 (2013)

71 (by July 2014)

The BSI Service Centre

Handling over 2 500 calls, e-mails and faxes every month, the BSI Service Centre plays an important role in the BSI's services to citizens. Opened in March 2014, the BSI Service Centre is available to callers free of charge at 0800 274 1000.

The BSI's new citizens' brochure

To coincide with Safer Internet Day 2014, the BSI has also produced a brochure on the cloud. Many IT users already use the cloud without even knowing it. The "Staying Safe in the Cloud" brochure is designed to ensure people are more knowledgeable about its use.

13. German IT Security Congress

Under the banner "Improving IT Security – Creating Trust in the Future", the 13th German IT Security Congress opened its doors in Bonn from 14–16 May 2013. Over three days, delegates from business, science and public administration learned more about current developments and trends in IT security.

The Information Security Journal

The official mouthpiece of the BSI is the <kes>, The Information Security Journal. This bi-monthly journal includes contributions from BSI authors on current issues related to IT security. The BSI element is supplemented by official information on certification. Alongside the print edition, the BSI <kes> forum can be accessed at **www.bsi.bund.de/ForumKES**.

The BSI makes contact with young people at an early stage through scholarships, university open days and fairs, internships and the supervision of theses.

The next generation

Across the board, employers in the IT sector (whether pulbic or private sector) find themselves suffering from a shortage of skilled workers. Graduates who leave university with good qualifications are in great demand on the job market. It is therefore important to attract the attention of talented young people and build ties with students whilst they are still at university.

The BSI has been offering scholarships to IT students in an attempt to attract them to join the organisation after graduating. The BSI accepts invitations to university recruitment fairs (such as the company day held by Bonn-Rhein-Sieg University and ITS-Connect, organised by Ruhr University Bochum). It also attends trade fairs such as CeBIT and IKOM as a way of making contact with potential young employees. Some courses include elements of practical work experience, which allow students to put their theoretical knowledge to the test in practice. During these internships, students assist the BSI in a number of different areas and often work on projects closely aligned with the subjects they are studying. These initial contacts (regularly involving various different departments and subjects) often lead to students subsequently asking the BSI to supervise their Bachelor's or Master's thesis. Every six months, a number of new topics are posted on the BSI website as potential subjects for internship reports or final dissertations.

Bachelors' and Masters' theses are supervised by experienced BSI staff members, who advise students over the course of a 3–6 month period and act as second assessors in the examination process. □

Bettina Westhofen,
Section
"Human Resources"

INTERVIEW

"PUTTING IDEALS INTO PRACTICE"

Mr Paegelow, you joined BSI in 2011 as a Media and IT graduate, and now you have official status as a civil servant. What motivated you to apply to the BSI?

During my studies the complex and fascinating topic of information security became less of a specialist concern and gained the attention of the IT world at large. I followed these developments with great interest. Fortunately I had an opportunity to learn more about information and IT security during my studies, mainly thanks to two compulsory options. This was quite unusual at universities at that time. Of course these courses introduced me to the BSI and its wide range of activities in the area of information security.

René Paegelow,
Section "IT Security Consulting for Public Authorities"

Were there any aspects which particularly attracted you?

During my work experience semester I carried out an audit of basic IT security at a medium-sized institution in line with BSI standards. This gave me an excellent insight into the complexity of information security. After finishing my internship, I was keen to continue pursuing the broad spectrum of IT security, so I decided to apply to the BSI to write my final thesis on "Developing basic IT security".

To what extent did this lead you to seek employment at the BSI?

I enjoyed writing my thesis at the BSI. I was supported by BSI staff from different departments under the general BSI premise that I had to carry out independent, high-quality work, contribute my own ideas and produce a thesis that would benefit the work of the BSI and the community as a whole. As a result, I was keen to work at the BSI after graduating.

What do you particularly like about the BSI?

Today I work in the BSI's Security Consulting unit and set myself the goal of always providing clients with ongoing, top-quality support. There are always new and fascinating challenges to tackle.

BSI staff

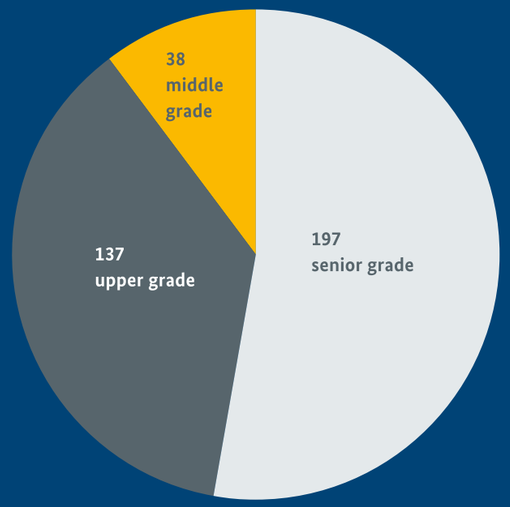
In 2014 the trendence marketing institute listed the BSI as one of Germany's top 100 employers.

trendence Graduate Barometer 2014 GERMANY'S 100 Top Employers

575 employees

7 trainees

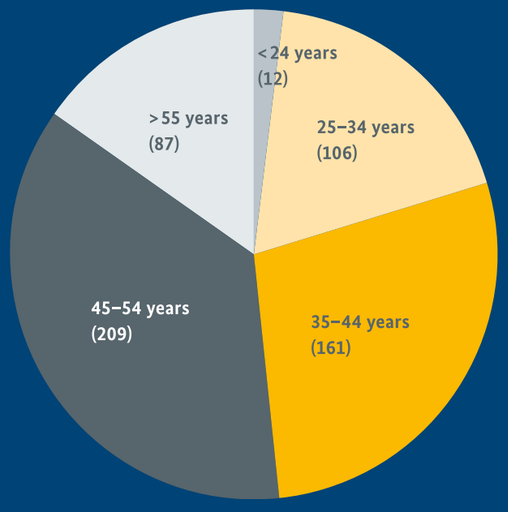
372 civil servants



Professional backgrounds

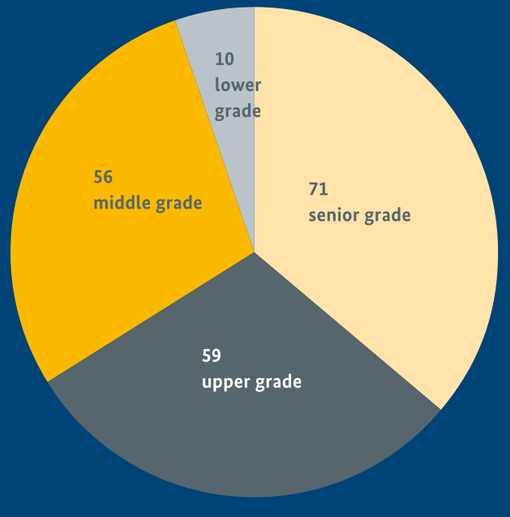
- 31 % engineers
- 22 % IT technicians
- 18 % administrators/ business managers/ financial managers
- 14 % mathematicians
- 11 % geologists, biologists, physicists
- 2 % lawyers
- 2 % other

Age range



143 women (24.87 %)
432 men (75.13 %)

196 employees covered by collective agreements



As at: 31.12.2013

2013

The BSI on the road

Edward Snowden's revelations, trade fairs, congresses and e-mail checks have all been major landmarks over recent months.

CeBIT

05.03. – 09.03.2013

CeBIT

CeBIT, the world's largest computer fair, is a fixture on the BSI's calendar. With a new stand design and a focus on cyber security and the Alliance for Cyber Security, initiated by the BSI and BITKOM.

08.04. – 12.04.2013

Hannover trade fair

Debut at the Hannover fair. Alongside the Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI), the BSI provided information on ICS and Industrial IT Security 4.0.

14.05. – 16.05.2013

IT Security Congress

Held on home territory in Bonn. Every two years, the who's who of the German IT security industry gathers at the German IT Security Congress.

June 2013

Snowden revelations

In June 2013, The Guardian and The Washington Post published secret documents that had fallen into the hands of former NSA contractor Edward Snowden. Snowden is now wanted in the USA on espionage charges.

October 2013

European Cyber Security Month (ECSM)

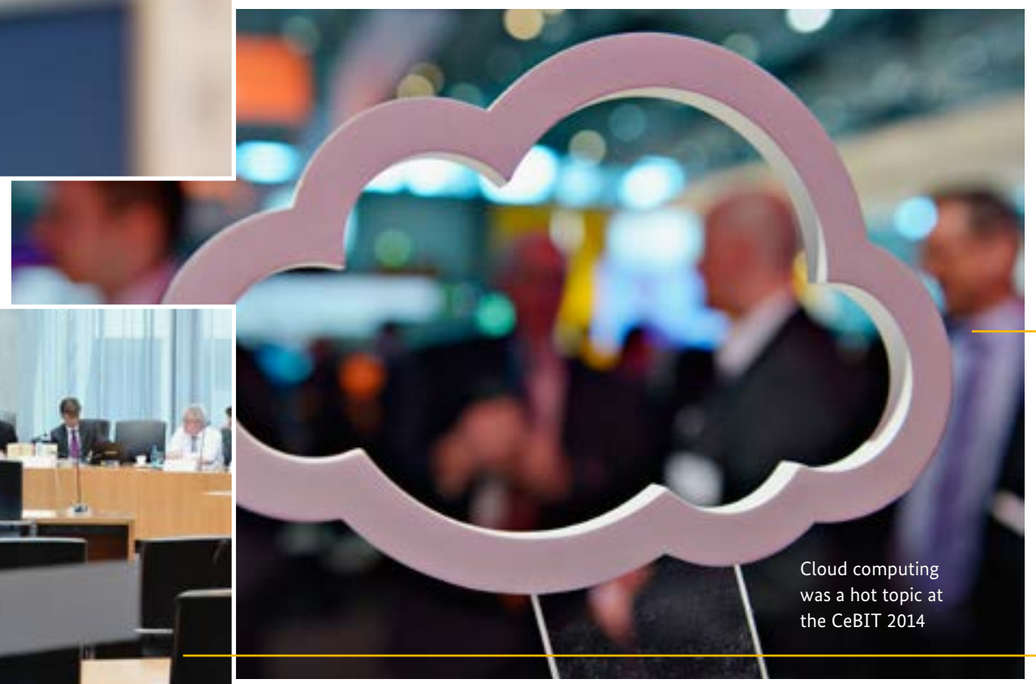
The ECSM is an EU campaign to raise awareness of cyber security. The BSI participated for the first time in 2013 with a series of promotions accompanied by social media on social networks, online shopping, mobile surfing and safe internet use.

15.11.2013

European Cloud Partnership (ECP)

The ECP Steering Board deals with strategic approaches to ensuring that public and private cloud services facilitate sustainable, innovative and economical growth. In 2013 the BSI organised the annual Steering Committee.

2014


Cloud computing was a hot topic at the CeBIT 2014

Berliner Forum Cyber-Sicherheit

21.01.2014

Mail checking

In the wake of a major incident of identity theft, the BSI set up a website for citizens to check whether they were affected.

22.01.2014

Forum on Cyber Security

The BSI organised the first Berlin Forum on Cyber Security in Berlin in conjunction with the Federal Academy for Security Policy. Representatives of business, politics and academia came along to discuss the future of IT security.

11.02.2014

Safer Internet Day

On the occasion of Safer Internet Day, the BSI published a citizens' brochure on the cloud and set up a special hotline to answer questions about cloud computing.

10.03. – 14.03.2014

CeBIT

CeBIT 2014 has a new look with a B2B orientation. This did not affect the flow of visitors to the BSI stand and to the BSI representatives in the Public Sector Parc.

20.03.2014

NSA Inquiry Commission

The German Bundestag set up an inquiry commission to look into the NSA affair. The commission will investigate the extent and background of the spying carried out in Germany by foreign intelligence services.

20.08.2014

Digital Agenda

The German cabinet agreed on the "Digital Agenda 2014–2017".

23.09. – 26.09.2014

security essen

security essen is the world's leading trade fair for security and fire prevention. The BSI is represented in the areas of material-based security technology and IT security consulting.

02.10. – 03.10.2014

Hannover celebrations

At a festival in Hannover to celebrate the Day of German Unity, the BMI, BSI and The Federal Agency for Civic Education welcomed visitors under the banner "Germany comes together on the web – safely!"

www.bsi.bund.de