Federal Office
for Information Security

Improving IT Security

BSI Annual Report 2010

De-Mail Services
Technical Background and Testing Infrastructure

Cloud Computing
A Challenge for Information Security

Critical Infrastructures
Threats That Go Beyond Traditional ICT Infrastructures

Improving IT Security

BSI Annual Report 2010

IT Security

IT Security is a generic term for a state of affairs in which information technology systems are free from risk or harm. Security can be achieved if dangers are identified and eliminated in advance. The key task is therefore to counter threats with appropriate protective measures and thus forestall any possible damage.

Adapted from an definition in Brockhaus

Hans-Peter Friedrich
Federal Minister
of the Interior

Dear Readers,

The Federal Office for Information Security (BSI) was established 20 years ago. Looking back, one can say that the decision to set it up was a very prescient one.

Today the internet has become an integral part of our daily lives. Not only has it changed the way we communicate, but it has also created new ways of working and living together. Internet-based business models play a key role in increasing productivity and achieving economic growth. And this development is by no means nearing its end: in the future we will see aircraft, medical devices, electricity meters and much more besides connected to the internet.

This will open up a whole host of new and exciting opportunities for citizens, businesses, industry and public authorities alike. The key to using cyberspace successfully is trust – trust in both the security and the availability of the internet, not only in Germany but worldwide.

Through its role as the central IT service provider both within and outside the federal administration, the BSI has become an important partner and, therefore, a trust-giver. Over the past few years we have increased the powers of the BSI and made it an important point of contact for national and international companies.

Internationally acknowledged as a competence center for IT security, the BSI will need to keep pace with the speed of innovation on the internet going forward. Informing people of the risks that are out there on the internet and responding rapidly to vulnerabilities that come to light will require the BSI to liaise even more intensively with other authorities and with businesses and industry both at home and abroad.

I hope you enjoy reading this report and that it will give you plenty of insights and food for thought on the subject of using cyberspace securely.

Berlin, July 2011

Hans-Peter Friedrich

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

Dear Readers,

The BSI is out of its teenage years. At 20 we are a relatively young authority, but because our theme of IT security is subject to a dynamism virtually unknown in other public institutions, our range of responsibilities has been expanding constantly ever since our early days.

The year 2010 was no exception, and the implementation of the BSI Act has taken us into uncharted territory. For many years the BSI had wide-ranging tasks but not many powers. With our new legal basis we are now much better equipped to act as a defense authority going forward. This is an important development, since security experts are finding their work turning increasingly into a race against highly professional attackers.

We are greatly encouraged by the fact that cooperation between IT manufacturers, providers and security experts is constantly improving. They have all recognized that working together can benefit everyone concerned, so IT security is constantly improving at the national and international level. It is not only the internet that breaks down boundaries: the ever increasing number of threats brings those involved closer together and heightens public awareness. One of the most noteworthy examples of this in 2010 was Stuxnet. This malware clearly illustrated that attacks are now being targeted very specifically at enterprise and process control software. Across the world, the word on everyone's lips was "cyberwar". This development is also being tackled in the political arena, and measures have already been announced. For example, April 1, 2011 saw the opening of the National Cyber Defense Center under the auspices of the BSI.

There were several other exciting events. The launch of the new ID card (nPA) on November 1 marked the provisional culmination of a technically and organizationally ambitious IT project that the BSI has been part of right from the outset, playing a major role in its success. The German De-Mail Act entered into force on May 3, 2011, paving the way for setting up a secure communication infrastructure for citizens, enterprises and public authorities.

But we cannot afford to rest on our laurels: we must keep the momentum going. My employees and I are doing just that, with the aim of making the networked world more secure for all of us. I am delighted to be able to give you an insight into the work of the BSI in this Annual Report 2010, and I very much hope you enjoy reading it.

Bonn, July 2011

Michael Hange

Page 13
A Holistic Approach to IT Security

Page 18
De-Mail Services: Technical Background and Testing Infrastructure

Page 26
Cloud Computing – A Challenge for Information Security

Setting The Course – Planning The Future

Shaping IT Security

Security for the Cyber World

Communicating – Mobile and Protected

Secure Electronic Identities

Tackling the Challenges Together

The BSI Turns 20

Setting the Course – Planning the Future

"We Can Play Our Role Much More Effectively Than Before."

The BSI Act in Practice

Interview with Horst Samsel, Head of Organization and Leader of the New BSI Act Project Group, and Fabian Hodouschek, Specialist and Member of the New BSI Act Project Group

The Act to Strengthen the Security of Federal Information Technology *(Gesetz über das Bundesamt für Sicherheit in der Informationstechnik)*, referred to as the BSI Act for short, entered into force on August 20, 2009. The new Act significantly widens the spectrum of the BSI's functions and powers. We take a look at the changes this has brought about for the BSI and how the legal framework was implemented in practice. As Head of Organization, Horst Samsel headed the New BSI Act Project Group and was in charge of implementing the legal requirements within the BSI. As a member of this project group, Fabian Hodouschek played a key role in its implementation.

Mr. Samsel, the new BSI Act marks a turning point in information security. Is this evident in the BSI's day-to-day work?

Samsel: Under the previous law, the BSI was very restricted in the action it could take in relation to cyber security and network defense. For example, everything we did was based on individual service agreements with the various authorities. The new BSI Act has given us much greater scope to protect the federal government's communications technology against risks and take appropriate technical measures. For example, we have established the malware detection system SES and the malware prevention system SPS. By deploying these systems on a legal footing, we can protect government networks even more effectively. The BSI's new legal powers enable us to act more independently than before and respond more effectively to changing threats.

Are politicians also more aware of the BSI's tasks now?

Samsel: Politicians are definitely much more aware of what we do. Section 5 (10) of the BSI Act requires us to report to the Bundestag's Committee on Internal Affairs on our Section 5 activities (protection against malicious software and threats to federal communications technology), for example. We have to report specific findings on the threat situation and attack

scenarios. Before 2009 the BSI was to a certain extent blindfolded and had its hands tied at the interfaces to the government networks. Now we are in a position to actually take action. This also brings the risks associated with IT and the internet more into the political spotlight.

"The BSI's new legal powers enable it to act more independently than before and respond better to changing threats."

Horst Samsel

According to Section 4 of the BSI Act, the BSI is the central reporting office for IT security. What does this mean in practice?

Samsel: We were able to translate the legal basis into practical procedures most quickly in this area. Government authorities now have a legal obligation to report IT security incidents to the BSI. In late 2009/early 2010 we presented an administrative regulation setting out these reporting obligations. The BSI's key task in this area is to keep the authorities free from harm by protecting their communications technology against risks. Without our protective measures, which help filter out spam from government networks, for instance, every government employee would have an average of 20,000 e-mails per month to deal with. Up to 99% of e-mails received by the federal administration are spam.

The law lays down very strict data protection requirements. How does that work in practice?

Samsel: The use of the protection systems is based on the data collection and use concept, which has been discussed jointly by the BSI's specialist sections, our Financial Affairs department and our data protection officer and verified by the Federal Commissioner for Data Protection and Freedom of Information. Our malware detection system (SES) automatically checks all e-mail traffic at the interface to the federal government's communications technology. The criteria governing who can gain access to the system are very tightly regulated. As per the legal requirements, the SES is set up in such a way as to keep the number of cases in which a person has to gain knowledge of the content of a communication to an absolute minimum. Such cases must be very precisely recorded and may only be approved by a BSI employee qualified to hold judicial office. We have put the highest possible level of controls in place to prevent unauthorized access, with a series of instructions and safety precautions for systems and staff.

Section 5 of the BSI Act was the subject of a constitutional challenge in mid-2010. How do you view that?

Samsel: The issue of potentially interfering with fundamental rights was discussed intensively during the legislative procedure, so the provisions of Section 5 are in fact very balanced. For the areas

"The need for personal certification is growing, partly as a result of other laws."

Fabian Hodouschek

of the BSI Act that could affect the privacy of telecommunications or the right of individuals to decide how much information is disclosed about themselves, regulations were developed to limit such interference to a necessary minimum.

The principle of proportionality has been taken into account here, and data are not used indiscriminately.

Section 5 Protection against malicious software and threats to federal communications technology

(1) In order to protect federal communications technology against threats, the Federal Office may

1. use automated processes to gather and evaluate log file data generated by operating federal communications technology as necessary to recognize, contain or remedy disruptions to or problems with federal communications technology or attacks on federal communications technology;
2. use automated processes to evaluate data generated at interfaces of federal communications technology as needed to recognize and protect against malicious software.

The BSI Act gives the BSI the power to warn businesses, industry and citizens about security vulnerabilities in products and services.

Hodouschek: We have also made good progress in implementing section 7, which deals with the subject of warnings and alerts. We have defined a detailed process which needs to be gone through before we can issue a warning about an IT vulnerability with relevance to the public. We also always liaise with the manufacturer of the product concerned.

How do manufacturers react to BSI warnings about their products?

Hodouschek: In 2010 we had to issue some warnings that were covered widely by the media. Naturally enough, the manufacturers of the products responded critically, but no one has as yet gone so far as to take legal action. As we inform the manufacturers up front, there were no cases of BSI warnings catching a manufacturer unawares.

Samsel: You can see by the manufacturers' reaction how important the BSI's powers under section 7 are. We can play our role much more effectively than before. Manufacturers took us seriously even before the new Act came into force, but now they are much more willing to work closely with us. We put that down to the fact that the BSI has been given teeth, so to speak. Manufacturers approach us and seek cooperation at a much earlier stage now. Stuxnet was a good example of this: we did not simply issue a blanket warning, but we coordinated our approach very closely and responsibly with the manufacturer.

The Federal Office shall promote information security. To do so, it shall perform the following tasks: [...] Advising and warning federal and Länder bodies as well as producers, distributors and users with regard to the security of information technology, keeping in mind the possible consequences of the lack of security precautions or of inadequate security precautions; section 3(1) sentence 2 clause 14.

In order to protect government networks, the BSI is empowered to define uniform and stringent security standards for all German federal authorities and even to commission suitable products if required.

Samsel: That is how section 8 of the BSI Act describes it. It also empowers the BSI to provide IT security products for the federal government.

With the federal government's IT investment program that is now under way, we have been able to roll out information security products like SINA, SiMKo and SecuVOICE throughout the federal administration. So we have been able to promote IT security across the board much faster and in a much more targeted way than if we had simply had a supporting role in these developments, or if we simply granted permits and certificates and the authorities had been responsible for implementing them themselves.

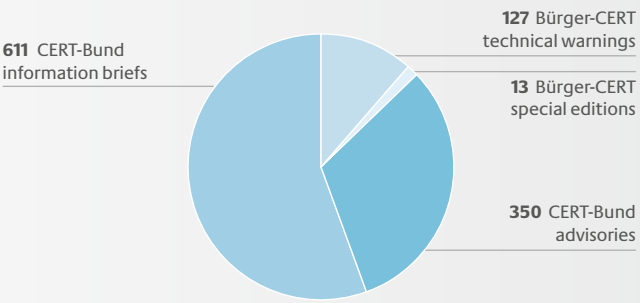
At present, we have 180 German authorities using SINA systems, and 23 are using the SINA Virtual Workstation. More than 30 authorities are using SiMKo.

In 2010 we worked very closely with the Procurement Office of the Federal Ministry of the Interior and signed a series of master agreements. These allow federal authorities to obtain products with IT security features as soon as they need them, and enable us to specify the IT security requirements they need to meet. We aim to further extend these master agreements going forward.

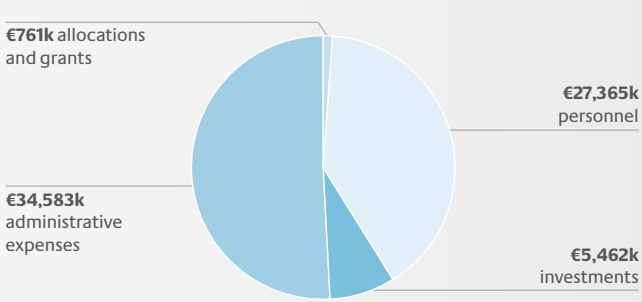
Does that not raise expectations on the part of manufacturers?

Hodouschek: Basically what we are doing is pooling demand, and that has an impact on the market. Ultimately we want to ensure that the federal administration can meet its need for products with appropriate security features.

CERT-Bund Warnings in 2010



BSI Budget Total 2010: €68,171k



Sure, manufacturers are going to have expectations – but these do not play a role in the choice of products.

How are these requirements accepted within the federal administration?

Samsel: Better than before. Many authorities tend to view IT security as something of a burden because it has a reputation for impinging on functionality and because of the many requirements that have to be met. Obtaining IT security products through a master agreement in which the BSI's standards are met is easier than having to go out and obtain the budget and resources themselves. This makes IT security more convenient. The reservations in terms of functionality and performance may not have disappeared entirely, but other negative constraints can be set aside. And this increases acceptance.

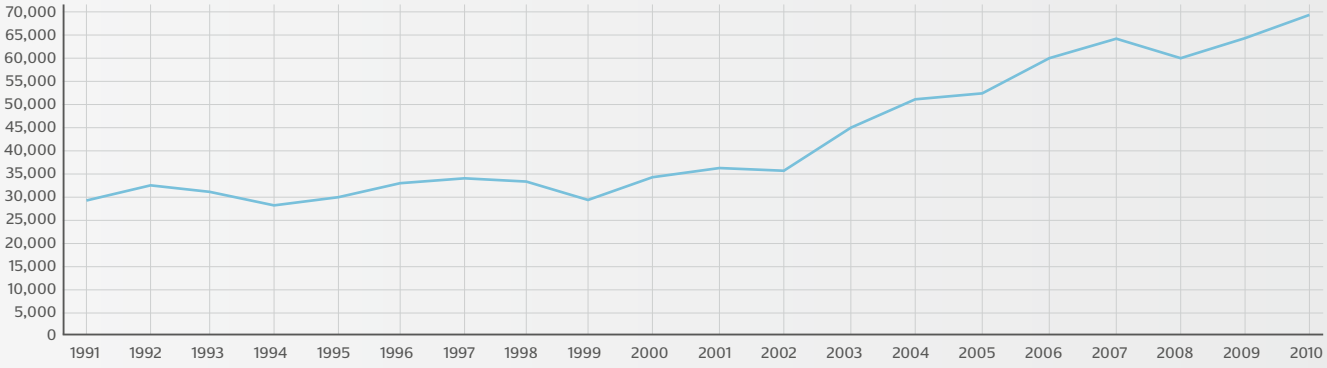
Since the introduction of the BSI Act, the BSI has also had the powers to certify people. How does this work in practice?

Hodouschek: Implementing personal certification is not a major issue, as the BSI has been active in certification for some time now and has certified people in the past. The processes are similar. The need for personal certification is growing, partly as a result of other laws that call for BSI certification. These cases are increasing, and the procedures are in place. In practice, therefore, this is not really a new issue for us. However, the way certifications are accepted by those on the outside is a constant learning curve. Although it has to be said that our past experience has been positive.

Do these extended powers also call for structural changes within the organization of the BSI?

Samsel: Obviously, changed tasks and new powers are bound to have an organizational impact on us. Further-reaching tasks make external interfaces more clearly visible. This is particularly true of the new powers under sections 5 and 8, which had not been clearly assigned within our organization before. We will be taking these into account in the reorganization of the BSI that is currently under way. There will be fewer changes in other areas that existed before the law was amended, such as CERT-Bund or accreditation and certification.

Development of Budget Total (in €k)



A Holistic Approach to Cyber Security

Dr. Hartmut Isselhorst, Head of Cyber Security

These days it is hard to imagine life without the internet. Everyone from young to old uses it for finding out information, shopping and banking online, e-Government, online gaming and social networking. Government authorities, businesses and scientific institutions all have websites on the internet and use it not only to offer their services but also as a communication platform and for mobile working.

Mass Attacks and Targeted Abuse

But the omnipresence of the internet has a downside. Our dependence on a properly functioning internet has risen exponentially: without it, many process chains would collapse. But as the internet's success has grown, so too has its attractiveness to crime and foreign state organizations hoping to possibly use it as a platform for

"We need to accept the challenge of 'cyber security for Germany' going forward."

Dr. Hartmut Isselhorst

terrorist attacks. The complexity of the software and the extent of the attackers' resources mean that they are able to find errors and vulnerabilities and abuse them for attacks via everyday internet services.

Examples include

- infecting websites with malware, so that simply surfing to these pages will result in a user losing control of their own computer (drive-by downloads)
- sending mass e-mails or even e-mails targeted to just a few select addresses with attachments containing manipulated files (Office files, PDFs, images etc) which can also lead to loss of control of the user's computer (Trojan horses)
- attacking large numbers of PCs worldwide, taking command of them and controlling them from a central point (botnets)
- sending out billions of unsolicited e-mails (Spam) via botnets which clog up countless servers
- using botnets to target and overload corporate and public sector servers and blocking their services (Distributed Denial of Service attacks – DDoS).

These mass and targeted attacks – also known as cyber attacks – lead to digital identities being stolen and abused, confidential information being mined, and IT-based processes being sabotaged.

Naturally, the federal administration is very much aware that it is exposed to all these new dangers. With the amendment of the BSI Act, the legislature has given the BSI the means to protect the federal administration by introducing central measures.

Measures to Protect the Federal Administration

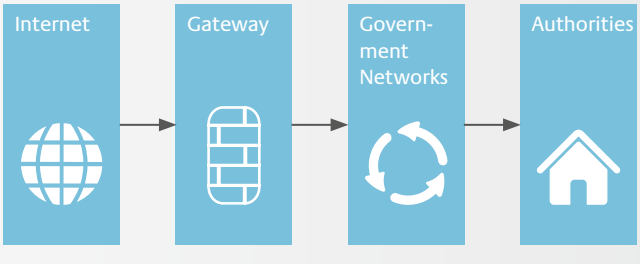
The BSI's cyber security strategy for protecting the federal administration is based on two main pillars:

- Identifying and fending off cyber attacks as early as possible and
- Using a staggered range of protective measures to confront cyber attacks.

The BSI's preferred holistic approach to cyber security implements this in four hierarchical defense areas:

- The internet itself
- Gateways between the internet and government networks
- Government networks
- Local networks and computer workstations.

"Four-Wall Strategy"



Cyber Defense Area #1: The Internet

The BSI's cyber security activities in relation to the internet itself can be divided into four areas. In the first area, "situation", the BSI CERT works with other national and international CERTs to identify, evaluate and resolve IT incidents. The associated Operations Center monitors the national and international IT situation and introduces crisis response mechanisms as and when necessary. It also issues public warnings about vulnerabilities and malware in accordance with section 7 of the BSI Act. In this area the BSI-CERT and the Operations Center work closely with operators of critical IT infrastructures in Germany. IT crisis exercises are held regularly to make sure all parties concerned can respond appropriately in an emergency.

In the second area, "internet infrastructure", the BSI works closely with internet operators, the eco-Association of the German Internet Industry and national internet providers to make the basic structures and internet services technically more secure. One example of this is the initiative to introduce the secure DNS service (DNSsec). The BSI also cooperates with global players on the product side to perform product security analyses and introduce security improvements before the product reaches the user.

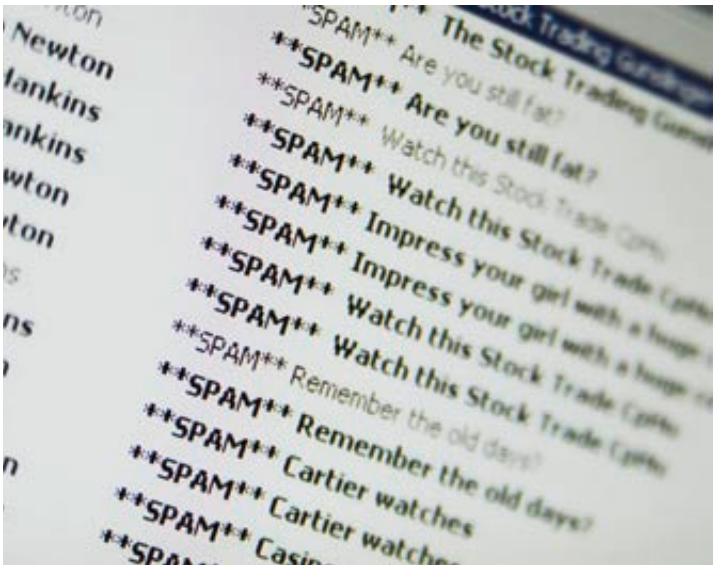
In the third area, "citizen", the BSI helps private users of the internet in Germany make their computers more secure. Botnets seek out unsecured private PCs and use them to create a virtual army for the cyber attackers' sabotage campaigns. The BSI runs the website BSI-fuer-Buerger, which provides information and tools and publishes Bürger-CERT warnings about the latest risks. In addition, the BSI also supports the provision of basic technologies for secure use of the internet, such as the new secure Digital ID card and the De-Mail concept for secure e-mail communication. If a private PC is captured and used as a bot for criminal purposes despite all the precautions, the user can turn for help to the Anti-Botnet Initiative run by the eco-Association of the German Internet Industry, which the BSI initiated and supports, and in which ISPs provide support for affected customers.

In the fourth area, "federal administration online", we can highlight two activities that make using the internet more secure for the federal administration:

- Security mechanisms have been agreed contractually with the ISPs of the government network that are designed to fend off or at least reduce the impact of a DDoS attack.
- As the federal administration's web servers are also attacked, selected government web servers are subject to permanent monitoring so that vulnerabilities or malicious software can be detected and eliminated as quickly as possible.

Cyber Defense Area #2: Gateway Between Internet and Government Network

At the interface between the government network and the internet, the BSI is responsible for traditional cyber security measures such as the spam filter, which weeds out more than 95% of incoming e-mails as spam, the cascaded virus filter, which identifies and eliminates widespread malicious software, and the firewall, which prevents conventional hacking attacks.



More than 95 per cent of e-mails are weeded out by the spam filter at the interface to the government network.

With its new powers under the amended BSI Act, the BSI can now take additional, more effective protection measures at this interface:

» The innovative Malware Detection System (SES), with which the BSI was able to identify and fend off more than 1600 targeted Trojan horse attacks in 2010.
» The Malware Prevention System (SPS), with which the BSI was able to block more than 300,000 access attempts on highly dangerous websites in 2010.

Cyber Defense Area #3: The Government Network

The government network between Berlin and Bonn, for which the BSI has security responsibility, has been hardened both in terms of availability and confidentiality. This includes making the network and its internet connectivity fully redundant. The fact that the government network only has two high-availability interfaces to the internet has proved to be a major advantage: the security of these connections can be closely monitored and they can be protected with the security measures mentioned above.

An additional security feature is the separation of voice and data transmission: if one channel fails, communication can still take place on the other. For confidentiality reasons, all communication on the government network is encrypted using cryptosystems developed by the BSI and authorized for use with classified state information. The final elements in the government network's security armory are permanent, redundant monitoring by the operators and the BSI's Operations Center. In addition, regular IT security audits and penetration tests are performed.

Cyber Defense Area #4: Local Networks and Computer Workstations

To protect the federal authorities' local networks and PC workstations, the BSI publishes recommendations such as the Internet Security series, the IT-Grundschutz catalogs and the High Availability Compendium. Another source of information is the alerts issued by the BSI-CERT, which the BSI Act has designated as the central reporting office for government security incidents. Additional services include security consultancy, penetration tests and IT security audits in the form of the Cyber Security Quick Check. The final line of defense is the provision of suitable products (firewalls, anti-virus programs, crypto products, secure USB sticks) and the design and development of cyber security products such as anomaly detectors, data transfer locks, secure surfing environments based on virtual systems, and secure solutions for mobile communication and mobile working.

Outlook

Having gained valuable experience and implemented cyber security successfully for the federal administration over the past two years, the BSI will need to continue to meet the challenge of "cyber security for Germany" going forward. In this field, it will need to open up new cyber defense areas and extend existing ones.

In Cyber Defense Area #1, The Internet, it will need to evaluate, monitor and fend off potential attacks on the internet infrastructure, especially attacks on DNS structures, attacks with manipulative routings and high-capacity DDoS attacks on national internet structures.

Cyber cooperation is an area that will take on great significance going forward. "Cyber security for Germany" can only be achieved if all players work very closely together. This includes:

» Cooperation with federal authorities actively involved in cyber security: the National Cyber Response Center is being set up in 2011 under the auspices of the BSI.

The BSI successfully implements cyber security

- Cooperation with ISPs: the BSI will be intensifying the cooperation that is already under way, working with ISPs to find ways of protecting private users' PCs on the one hand, but also to work out options to cope with a cyber sabotage attack on a national scale on the other.
- Cooperation with manufacturers of cyber security products and system houses: the BSI will work with the manufacturers to develop suitable cyber security solutions, initiate services and encourage relevant providers to do so.
- Collaboration with the private sector: to rehearse cooperative processes for national cyber defense, an exercise involving the federal government, Länder and operators of critical infrastructures in the private sector is planned for the end of 2011 (LÜKEX 2011).
- International cooperation: cyber aggressors (cyber criminals, cyber spies, and cyber terrorists) are an international phenomenon. To respond to them, intensive international cooperation is needed with a view to exchanging experience, knowledge and best practices ahead of such occurrences and to facilitate concentrated defense in acute attack situations.

To promote cyber security in the private sector, the BSI will be helping businesses and industry to help themselves. Three areas are currently planned:

- Best Practices: the BSI will be working with the private sector to develop best cyber security practices, focusing on cyber sabotage and cyber espionage protection. It is planned to make the results and experiences available on a new cyber security web portal.
- Training Center: a training center is currently being set up, where IT administrators will be trained in fending off cyber attacks. Initial thought is being given to making this facility available to the private sector as well.
- Certification of cyber security consultants and service providers: demand for specialist consultants and service providers will increase in the future. Under the amended BSI Act, the BSI is authorized to accredit and certify suitable providers.

Facing New Challenges

The next challenge is already on the horizon. Today the internet is a platform that is predominantly used by PCs and smartphones. But tomorrow the internet will be ubiquitous and will pop up in all manner of new areas: vehicles and aircraft will be connected to the internet, medical devices in doctors' surgeries and hospitals will need internet access for maintenance, and electricity meters and control technology will have internet access. So malfunctions will have the potential to cause massive harm and even risk to life and limb. And finally, our dependence on the internet functioning efficiently will also increase with the growth of cloud computing. Cyber Security 2.0 will also only be able to be achieved holistically and with the cooperation of all concerned.

Shaping IT Security

De-Mail Services: Technical Background and Testing Infrastructure

Dr. Astrid Schumacher, De-Mail Project Manager, BSI

De-Mail enables documents and messages to be sent confidentially and reliably via the internet. It increases the security of electronic communication, giving the De-Mail account holder maximum security with minimum effort.

The De-Mail project – a successful joint venture

De-Mail
So einfach wie E-Mail, so sicher wie Papierpost.*

* As easy as e-mail, as secure as the conventional post

The De-Mail project is being implemented under the auspices of the Federal Ministry of the Interior. The BSI is responsible for its technical implementation, including the development of the Technical Guideline on De-Mail with individual modules on the various obligatory and optional services.

The De-Mail project is part of the federal government's modernization program, “Network-based and Transparent Administration”, and is consistent with the National e-Government Strategy. Among its long-standing supporters are associations such as BITKOM and the 3rd Working Party on Innovative State IT Services, which was set up during the National IT Summit. Large numbers of SMEs, banks and insurance companies took part in the pilot project, since the availability of a confidential and reliable electronic communication channel is very important in their areas of business. Following positive feedback from test users and given the high demand for this service among companies and public authorities, the providers involved in the pilot scheme have continued to operate their De-Mail systems ever since. In addition, they are also implementing industry projects in which the parties involved can learn about De-Mail and practice integrating it into their internal IT systems and underlying business processes.

Better safe than sorry: De-Mail enables documents and messages to be sent confidentially and reliably via the internet.

Encrypted - Authentic - Demonstrable

The main security goals of confidentiality, integrity and authenticity in De-Mail communication are guaranteed with the security measures defined in the De-Mail Act.

The Act Regulating De-Mail Services and Amending Other Provisions *(Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften)*, which entered into force on May 3, 2011, provides the legal basis for the BSI as the competent authority for the accreditation and authorization of De-Mail providers. Now that the Act has become law, De-Mail can be rolled out. De-Mail enables the identities of the parties to the communication and the delivery of the De-Mail to be proved. The contents of a De-Mail cannot be intercepted or changed on its journey through the ether.

De-Mail service providers must enable every user to log onto their De-Mail account securely using two separate security devices such as possession (a token, e.g. the new ID card or a mobile phone) and knowledge (a password or a PIN). De-Mails are encoded during transmission and cannot therefore be intercepted or manipulated by third parties. If end-to-end encryption is also required, users can encrypt the contents of a De-Mail themselves. De-Mail makes this easier by obliging providers to publish the necessary public codes in a directory service at the user's request. The integrity of the contents of messages in a normal De-Mail communication is already protected as standard with a secure hash function. In addition, the provider attaches a qualified electronic signature to all delivery and read receipts. If a user wants to sign every message with a qualified signature as well, they can add their own components. This system effectively blocks spam, as senders of De-Mails are clearly recognized via the secure initial identification. The new electronic ID card can also be used for this purpose.

The Technical Guideline on De-Mail

BSI Technical Guidelines are a proven means of providing users and manufacturers with technical specifications in a standard format. They enable users to select tested products for a particular use, and manufacturers can build their products according to the recommendations in the guidelines and have them checked for conformity with the specifications.

De-Mail providers are required to meet high standards in terms of security, functionality and interoperability, which are set out in detail in Technical Guideline 01201 De-Mail. In 2010 the BSI focused attention on further refining the technical background and accreditation infrastructure in the individual modules of the Technical Guideline and supporting the legislative process. Once again, the future De-Mail providers who were already involved in the project took part in 2010. The BSI has published the criteria on its websites ever since the project was launched. The latest version of the Technical Guideline is also available online. Additional information can be obtained directly from the BSI by e-mailing de-mail@bsi.bund.de.

BSI TR 01201 De-Mail provides the overall framework for proof of functionality, interoperability and security. It also describes the requirements De-Mail services must meet and the requirements for verifying these properties (test specifications). The TR has a modular structure reflecting the various services in the De-Mail setup.

It consists of the following modules:
» IT Basic Infrastructure
» Account Management
» Mailbox and Delivery Service
» Identity Confirmation Service
» Document Store
» (Higher Level) Security
The relevant areas of compliance for each service are functionality, interoperability (for the basic infrastructure, mailbox and delivery service, and identification service) and security.

Accreditation requirements

The main areas regulated by the De-Mail Act are the accreditation requirements and the documentary evidence showing that these requirements have been met. For example, it specifies exactly how future De-Mail service providers must prove that they meet all the technical and organizational requirements for providing the various services. This includes certain security services for the De-Mail account holder, such as checking every outgoing message for viruses, Trojan horses or other malicious software, that are run automatically every time a message is sent. Precisely defined and comprehensive security mechanisms form the core of the security requirements a service provider needs to meet in order to protect the De-Mail data and the communication itself. The mandatory requirements also include obligatory penetration tests and an IS audit. Providers must establish an information security management system in which the baseline protection measures are monitored regularly to ensure that the defined security targets can be met on an ongoing basis in the light of the threats.

Proof of compliance in the areas of functionality, interoperability and security is provided in the form of certificates from IT security service providers who must be certified by the BSI. The technical and personnel requirements that need to be met for certification are defined in BSI process descriptions.

De-Mail Test Centers and Auditors
A number of auditors and test centers have obtained BSI De-Mail certification or authorization to enable them to test De-Mail service providers.

De-Mail auditors can perform ISO 27001 audits on the basis of IT-Grundschutz and the specific De-Mail requirements set out in TR De-Mail. This mainly concerns the higher level security requirements that apply to all De-Mail services.

De-Mail test centers can perform functionality and interoperability tests in accordance with TR De-Mail.

A list of current certified De-Mail auditors and authorized test centers and their areas of authorization can be found on the BSI website: www.bsi.bund.de » Topics » Certification » Technical Guidelines » Certification according to Technical Guidelines » Accredited evaluation facilities (in German).

Providers looking to operate as a De-Mail service provider must submit their audit and test reports to the certified De-Mail IT service provider, who will issue the certificates required for accreditation.

Shaping IT Security as a Factor For Success

Günther Ennen, Head of IT Security Advice, BSI

Information and Communication Technology (ICT) is an indispensable core element of almost all business processes, whether in the public, private or research sector. The race to make technical systems ever more powerful and storage volumes ever bigger defines competition in the marketplace. The new opportunities offered by modern IT are driving providers and users alike to the limits of what is possible. The result? Time-critical processes with often sensitive information in increasingly complex network structures are shaping how people and organizations work together – wherever they happen to be in the world. IT security, or information security in general, is a process that assesses the need to protect information, examines the reliability of the technology, recommends protective measures and therefore generally helps to make IT services more reliable.

Security Requirements for IT Operations

In general terms, reliable IT operations need to meet the following requirements. The technology and applications must operate uninterrupted (availability), the systems and data must be flawless (integrity), and the information must be protected against abuse (confidentiality). However, the demand for reliable IT operations also brings with it risks which we are only partly aware of because of the quantity, quality and complexity of the objects involved. The risks are manifold, ranging from accidental human error, technical faults and force majeure through to intentional, large-scale criminal attacks. What is more, the risks can come from anywhere on existing networks. This risk situation shows that IT security is not an isolated process. So the requirements and protection measures must be analyzed and implemented in conjunction with other corporate goals (e.g. functionality, efficiency, flexibility, compliance and resilience).

"IT security is not an isolated process, and the requirements must be analyzed and implemented in conjunction with other corporate goals."

Günther Ennen

While the importance of IT security is never in doubt, often we will not be actively aware of the need for it until after a security incident has happened. The cost of rectifying the damage caused – for purging systems and databases after a malware infection, for example – is hard to estimate. Security incidents can, however, also lead to financial losses which are easy to quantify: quite apart from the issue of lost profits, companies are increasingly taking out IT service contracts with Service Level Agreements (SLAs) which not only regulate liability but also include contractual penalties for non-performance or loss of production.

Information Security Management Systems (ISMS): Shaping and Controlling IT Security

The process of operating IT is virtually always subject to rules and regulations. These call for control mechanisms, whether in the form of a periodic obligation to report, documentary evidence of regular IT operations or a detailed description of the entire risk management system. However, these mechanisms are only a small part of a comprehensive information security management system. The much-cited quote by US computer security expert Bruce Schneier sums it up nicely: "IT security is not a product, it's a process." It therefore has to be constantly developed and adapted. Thus IT security is subject to a special dynamic and is also always a function of time. The individual elements that go together to make up IT security are subject to constant change. Staff come and go, and technologies are constantly updated, enhanced or undergo quantum leaps. Information security management therefore plays a very important role. It covers a large area of responsibilities and activities on the IT security map. It initiates, controls and manages the IT security process on behalf of the organization's management.

The first and often the hardest step is to convince users of the need for IT security. Attitudes towards working out a professional IT security strategy are often colored by preconceived ideas: IT security takes time, costs money and causes performance loss, placing a big question mark over its financial viability. What is more, the immediate impact of IT security is neither visible nor tangible. Therefore, information security management always resides in the area of tension described by the Maximin principle: maximizing risk reduction with minimal use of financial and human resources. The availability, integrity and confidentiality of business processes must be protected and stabilized in such a way that significant risks are eliminated or at least kept within tolerable limits. To guarantee the reliability and confidentiality of an IT system, the following spheres of action are recommended:

- **Sphere of Action #1: Human resources.** Selecting personnel, documenting expectations, parameters and instructions, and updating them regularly.
- **Sphere of Action #2: Organization.** Documenting responsibilities and procedures, from the design stage to monitoring target achievement. The access processes and proof of access are defined on the basis of the need-to-know principle.
- **Sphere of Action #3: Technology.** Implementing strong processes for access protection, identification, authentication and reporting. Encryption mechanisms that enable the information to be appropriately protected.
- **Sphere of Action #4: Infrastructure.** Selecting suitable premises for IT operations, meetings and archives, access control and monitoring.

With a view to ensuring continuity of business processes, this sphere of action reveals an area of tension between functionality, effectiveness, efficiency, flexibility, compliance and resilience.

- Efficiency focuses on optimizing costs with an acceptable cost/benefit ratio.
- Flexibility is the foundation for long-term competitiveness and enables organizations to respond to constant technological change.
- Compliance is informed by rules and regulations designed to ensure correct operation.
- Resilience focuses on the organization's ability to survive by minimizing risks while ensuring maximum continuity of business processes.

Shaping IT security is not an end in itself. Defining security goals, analyzing the risks and understanding the legal requirements curtail the overall scope for action that represents adequate IT security.

Working Towards IT Security with Standards and Certifications

Over the years, large numbers of standards and best practices have been developed with this in mind. Certificates and standards are used to verify the current status of IT security in an organization's own area of responsibility. Experience shows that it is sensible to use established process models for this purpose. Among the reference models are the best-known exponents of IT-Grundschutz and the CobiT (Control Objectives of Information and Related Technology) and ITIL (IT Infrastructure Library) process models. The PDCA (Plan, Do, Check, Act) circle has established itself as an approach to shaping and delivering IT services. If similar quality levels need to be evidenced, we recommend opting for certification according to international standards such as ISO 27001.

Audits and pen tests can give rise to measures which should be prioritized and implemented by ranking and comparing their risk minimization effects and resource effort. At the same time, they enable the organization to produce an up-to-date estimate of the risk and security situation of all the information that needs to be protected. In order to keep the security process effective and efficient, it is sensible at this point for the IT security team to coordinate all activities with the organization's management, in order to close the PDCA circle.

IT Security, Economy and Resilience Go Hand-in-Hand

The demands for functionality, effectiveness, efficiency, flexibility, compliance and resilience describe an area of tension with apparently conflicting goals. One that is made worse by minimal or ever scarcer financial or human resources. Such conflicts can be resolved with IT governance models which enable an organization to introduce and professionalize its IT security management. Very often it is necessary to convince the organization's management by providing a cost/benefit comparison. Experience shows that finding funds for external consultants, security products or services is often less of a problem than releasing people in-house to take up full-time or team roles as IT security officers. Either way, costs are incurred, and in information security you always have to pay once: either before the crash or afterwards!

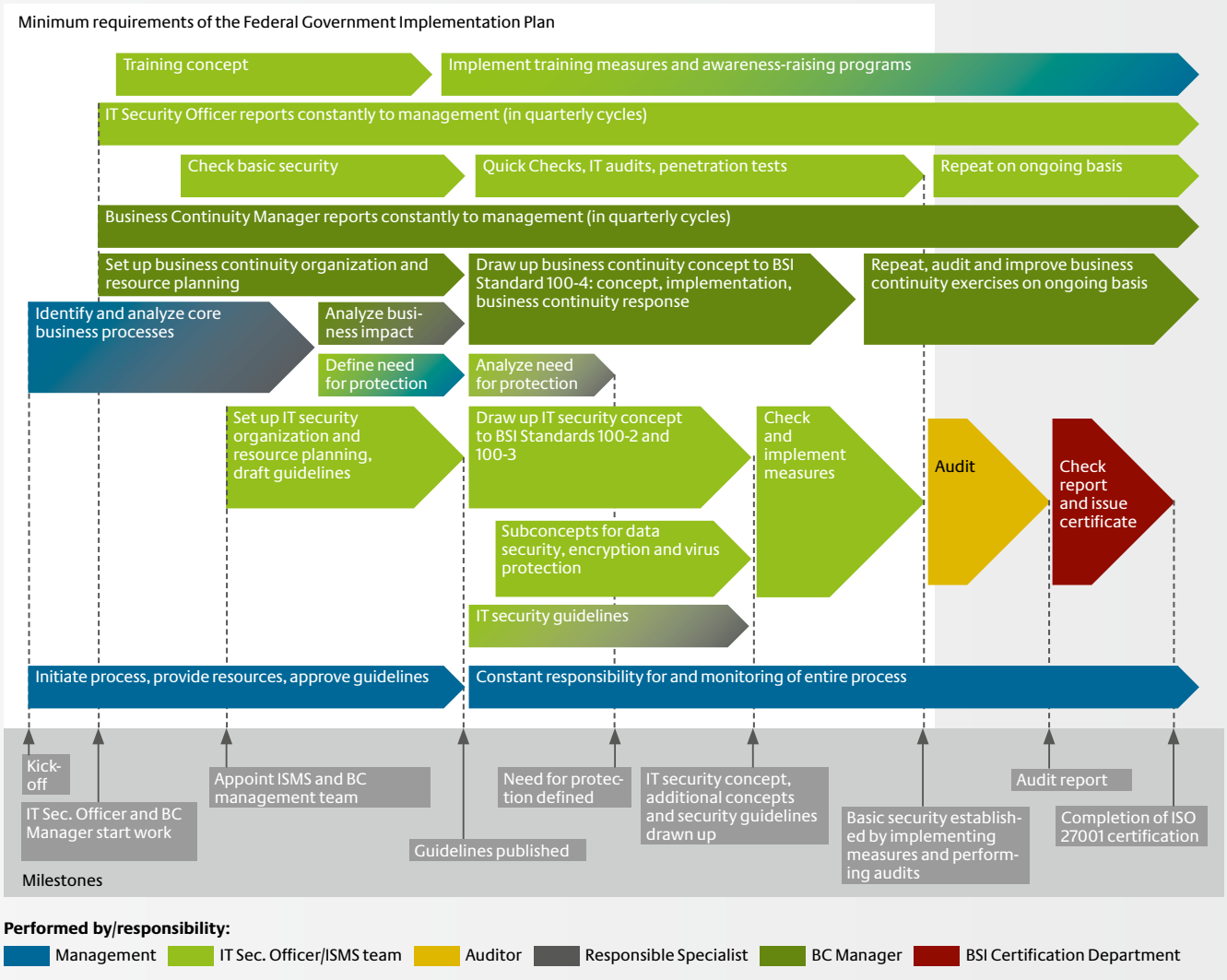
What Needs Protecting? Where are the Crown Jewels?

If IT security is to be shaped effectively and economically, it is important to take a close look at the extent to which information, applications and IT systems need to be protected. You cannot decide exactly what needs to be prevented at all costs and what needs to be protected without knowing what and where the Crown Jewels are. The definitive answers must come from the organization's management and will serve as the cornerstones of the risk prevention strategy.

Shaping IT security is not an impossible challenge. It is less a question of ability and more a question of a lack of will to deal with the tasks.

It is important to get the message across that the process can be shaped in every phase and to a highly effective extent – always within the confines of what is possible at the present time. The security of the technology and business processes the responsible people are in charge of is an asset in itself, because it impacts directly on their own sense of security. Media coverage of attacks on IT, technical system failures, unreliable communication channels, new malware, sophisticated fraud attempts or hit-and-run-style insider threats are extremely unsettling for the organization's security managers. Knowing that "these incidents can't happen on my watch" gives the people concerned peace of mind, and lays the foundation for successful business operations, both in the private and public sectors.

Roadmap and Responsibilities for ISMS and BCM*

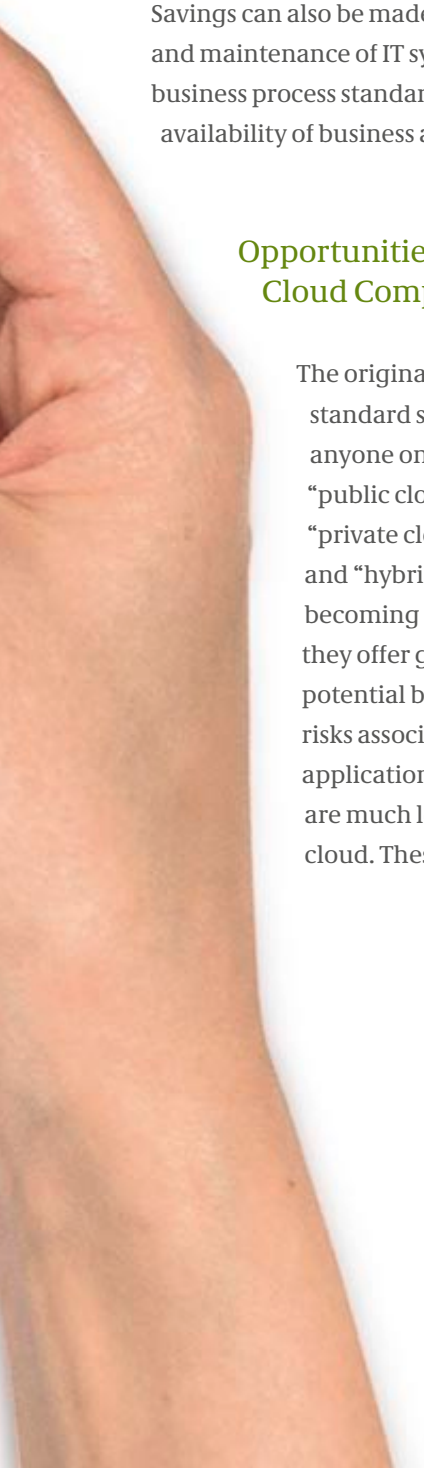


* Business Continuity Management

Source: BSI

Dr. Clemens Doubrava and Alex Didier Essoh,
Specialists in IT Security Management and IT Grundschutz, BSI

The subject of cloud computing has gained markedly in significance worldwide in recent years and was voted IT Trend of the Year in 2010 and 2011[1]. Market researchers expect expenditure on cloud services in Germany to grow rapidly over the next few years. It is estimated that sales of cloud services alone in Germany will rise from €1.14 billion in 2010 to as much as €8.2 billion by 2015. This corresponds to an average annual growth in sales of 48 per cent.[2]



There are many reasons why interest in cloud computing and the use of cloud services are on the rise. Cloud computing is a model in which IT services such as processing capacity, external storage, development and runtime environments, application software or even entire working environments are offered on the net, enabling IT services to be bought, used and stopped as and when required and paid for according to actual use. Savings can also be made on the acquisition, operation and maintenance of IT systems. Other benefits are business process standardization and the ubiquitous availability of business applications.

Opportunities Versus Risks of Cloud Computing

The original concept of the "cloud" – standard services that can be used by anyone on the internet – is known as a "public cloud". Other cloud models are "private clouds", "community clouds" and "hybrid clouds". Private clouds are becoming increasingly popular because they offer greater control. But besides the potential benefits, there are also various risks associated with having data and applications hosted in a public cloud that are much less likely to occur in a private cloud. These include the following:

- Outsourcing IT to a public cloud means that the cloud customer is heavily dependent on its cloud service provider, as it no longer has direct access to the hardware and software.
- Large numbers of unknown users share a common infrastructure, which increases the risk of the underlying values of information security (confidentiality, integrity, availability) being compromised.
- Data and applications are accessed via the internet, so they are inaccessible if the internet connection fails.
- As resources become more concentrated, Distributed Denial of Service (DDoS) attacks on cloud computing platforms are likely to increase.

Some of the above risks, such as DDoS, are not specific to cloud computing but are amplified because of the environment in which the functions are used.

Alongside technical and organizational issues, there are also legal aspects of cloud computing to be considered. In this context there are a series of questions that need to be answered, such as: Which country's law is cloud-hosted IT subject to? Where is the data, and is it adequately protected against access by third parties, e.g. state agencies? What happens if the cloud provider goes out of business?

How the BSI Is Increasing Information Security

Despite the fact that we are seeing an increase in the uptake of IT cloud services worldwide, almost all surveys and studies show that there are also many obstacles stopping us from using them even more. One of the biggest of these is the lack of information security. To address this issue, and to support both users and providers of cloud services, the BSI has initiated a series of measures.

[1] BITKOM press release, January 18, 2011
[2] BITKOM press release, October 6, 2010

Alex Didier Essoh and Dr. Clemens Doubrava, Cloud Computing Liaison Officers, BSI

BSI White Paper: Minimum Security Requirements for Cloud Computing Providers

On September 20, 2010, the BSI published a White Paper entitled "Minimum Security Requirements for Cloud Computing Providers" as a draft for discussion. This paper looks at how information with a normal to high protection requirement is processed in the cloud, and categorizes the data according to their need for protection in line with BSI standard 100-2.

The White Paper forms a basis for dialog between cloud providers and cloud customers, with the aim of developing meaningful and appropriate security requirements for cloud computing that guarantee protection of data and systems.

It discusses fourteen areas of cloud computing security that have been identified as critical (referred to as "guidelines") and contains a series of best practices (or "minimum security requirements") for dealing with the areas addressed. Another guideline describes additional requirements for cloud computing providers from the federal administration's point of view. Alongside security requirements in traditional areas of IT, such as security architecture, ID and rights management, business continuity management and monitoring and security incident management, the White Paper also discusses issues with particular relevance to outsourcing data, applications and processes to a public cloud. These include transparency, contract wordings, data protection and multi-tenancy. Ensuring that the tenants using the shared IT infrastructure are securely and reliably isolated from each other is a key aspect of security in cloud computing.

The White Paper was discussed at length and constructive comments were put forward. The suggestions were incorporated into the final version of the BSI's Minimum Security Requirements.

"Cloud Computing is a paradigm shift in IT towards more service-oriented services that are offered and consumed via the internet. This is equally important and attractive for both customers and providers. Besides the economic advantages of the cloud, such as economies of scale and flexibility, security is a key theme. Security is of paramount importance if cloud computing is to succeed in the market. The BSI addressed the issue of security in the cloud at an early stage and has been in dialog with the industry on this subject for some time. Microsoft welcomes the many opportunities for constructive, critical discourse on security in the cloud that the BSI has provided in various workshops and one-to-one meetings. This fact, along with the recently published White Paper on minimum security requirements in the cloud, is informing the discussion around information security in the cloud in a positive way. From our perspective, the work the BSI is doing around security in the cloud is going in exactly the right direction. Security in the cloud is just as important to Microsoft as it is to the BSI, and we look forward to continuing to work closely and constructively with them going forward."

Gerold Hübner, Government Security Director, Microsoft Corporation

Right from the outset, EuroCloud Germany_eco has focused on the security and trustworthiness of cloud computing. We have taken a major step forward in this area with the development of the certification system for Software as a Service, EuroCloud Star Audit SaaS. Our close collaboration with the BSI has been particularly important. Not only has it enabled us to offer high-quality certification, but it has also given us the opportunity to input the experiences of cloud providers into the work being done on the BSI minimum security requirements. We have very much appreciated the BSI's willingness to engage in constructive dialog on the definition of the underlying conditions. Cloud computing will continue to develop at a tremendous pace in the future. It is therefore important to formulate requirements on security, data protection and interoperability at an early stage. The cloud providers are extremely happy to support this process and to be able to demonstrate that they have put all the necessary measures in place to offer secure cloud services. We look forward to continuing to work with the BSI on shaping cloud computing with "Security – Made in Germany".

Andreas Weiss, Director Eurocloud Deutschland_eco e.V.

Study: "Development of Security Recommendations for Cloud Computing"

Alongside the minimum security requirements, the BSI is conducting a study on the "Development of Security Recommendations for Cloud Computing". This document is based on publicly available information, a workshop with key stakeholders and many subsequent interviews with both cloud providers and cloud enablers on the security functions on their platforms. The central aim of this study is to gain insight into the internal processes, procedures and principles of cloud service providers. The results of the study will be incorporated into the BSI's minimum security requirements for cloud computing.

Short Studies on the Private Cloud

To be able to exploit the potential benefits of Cloud Computing while retaining control over their IT infrastructure, many users turn to their own virtualized data centers to provision services. In this case too, technical, organizational and infrastructure measures need to be put in place to ensure that the services can be operated and used securely. Against this backdrop, In November 2010 the BSI initiated a series of short studies focusing on private clouds in conjunction with cloud technology providers. The aim of these short studies is to conduct a detailed, in-depth security analysis of cloud computing systems, their primary aim being to draw up security recommendations for secure private cloud computing. The studies are only looking at private cloud implementations offered as infrastructure packages, in other words integrated, tested and validated IT systems consisting of server, network, storage and management components. These integrated or converged environments are increasingly being advertised as "Cloud in the Box". The results of the short studies will be published in 2011.

Integrating Cloud Computing in IT-Grundschutz

The results of these short studies will be incorporated into IT-Grundschutz. The BSI plans to develop IT-Grundschutz modules for both using and providing cloud services. BSI standard 100-2 will be adapted to reflect the integration of cloud aspects into the IT-Grundschutz methodology. The modeling of complex, virtualized information networks may also make it necessary to adapt the GSTOOL.

Threats That Go Beyond Traditional ICT Infrastructures

Stefan Ritter, Head of CERT-Bund and Hans Honecker, Critical Infrastructure Protection Specialist, BSI

In 2010 the emergence of Stuxnet highlighted just how serious IT threats that go beyond traditional office communication and data processing have become.

Using ICT Beyond Traditional ICT Infrastructures

The days are long gone when standard information and communication technology was only used in traditional infrastructures like office communication environments, data centers or communication networks. Modern infrastructures in areas like utilities and manufacturing, finance, healthcare and business are increasingly built with standardised IT components whose basic features resemble traditional IT or that are based directly on normal commercial technology like PCs, conventional network technology or standard applications.

This is particularly true of critical infrastructures that provide essential services for the community, business and industry.

Despite being based on traditional IT components, these special technologies are designed specifically for the application in which they are used. Components in systems controlling physical manufacturing processes are very different from control components in the energy supply sector.

And neither of these has much in common with complex medical devices. In addition, within the individual areas of use, the specific features of the physical, technical and IT components differ widely from one installation to the next – for the simple fact that product lines from different manufacturers are used, and systems' ages differ.

Stuxnet – Targeted Attack on Process Control Systems

With its exposure in 2010, Stuxnet attracted considerable public attention. It is a highly complex and thus development-costly piece of malware that targets industrial process control systems. As expert analyses have revealed, Stuxnet is programmed to sabotage a particular facility cofiguration in a highly sophisticated and subtle way. It uses IT resources to target a specific process control technology and manipulates the processes by monitoring certain variables and changing control commands without the system operator noticing. A successful attack could render the product being processed unusable or even destroy the production systems.

Targeted Attacks Threaten ICT-based Special Technologies

The main concern in the public debate around Stuxnet was the vulnerability of critical infrastructures. Under the surface, however, Stuxnet is in fact less significant as a piece of actual malware; rather, its relevance lies in the fact that it clearly demonstrates the potential of attacks of this quality. It proves that there are people out there who spare no expense or effort to attack what they perceive to be key targets and sabotage them unnoticed. However impressive the complexity and technical quality of the Stuxnet attack may be, there is no reason to assume that such attacks can only be executed by the originator of Stuxnet, nor that Stuxnet was and will remain the only attack of this quality. What is more, the changed quality of the threat will not be restricted solely to physical process control technologies. Instead, we must now assume that IT-based special technologies in general are under threat from targeted attacks. We need to re-evaluate the risk of such targeted attacks on process control systems or other IT-based special technologies – both in critical infrastructures and in general use.

"A successful attack could render the product being processed unusable or even destroy the production systems."

Stefan Ritter

Hans Honecker

Non-targeted Attacks Pose Growing Threat

Alongside targeted attacks executed with a high degree of complexity, non-targeted attacks and rogue threats from stray malware are posing a growing risk to IT-based special technologies. For example, Conficker, a non-targeted, aggressively propagating worm, has the potential to cause serious disruption with severe consequential damage.

Dealing With the New Threats

Beyond the traditional IT setting too, severe disruptions caused by traditional IT attacks and stray rogue malware need to be considered as risks. This is nothing new in areas where IT security is already implemented consistently, but last year's incidents once again highlighted the need for action in areas where it is not. However, it is particularly important to re-evaluate the risk and potential harm of targeted, high-quality and elaborately executed attacks on IT-based special technologies regardless of their existing IT security status. Depending on the specific process architecture requirements and the special technologies being used, it may be necessary to implement highly specific measures to prevent these new threats from turning into unacceptable risks.

Critical Infrastructures

Both the state and the operators of critical infrastructures have taken these threats to IT-based special technologies into account for many years. Risk assessments already take account of the development of the threat brought to light by Stuxnet in abstract terms. Operators of critical infrastructures in particular have the necessary resources in place and can therefore respond quickly to new IT threats. In addition, as part of the joint measures for protecting critical information infrastructures, the state and the operators have been working closely together for many years. This collaboration was further intensified in recent years.

Critical infrastructure operators in several industries and sectors in Germany have set up additional Single Points of Contact (SPoC) for exchanging relevant information, alerts and situation updates with the BSI Situation Center. This communication between state and operators came into its own last year, both in some actual security incidents and in regular exercises. As a result, some key aspects of the 2008 joint communication concept[3] have been fleshed out over the past two years – not only through general collaboration but also through concrete measures that include establishing operational communication mechanisms for prevention in the new situation and coordinated mitigation of IT crises. So we now have a good basis in place for maintaining the necessary level of security for IT-protected special technologies in critical infrastructures. This should enable us to jointly and effectively combat potential IT-based attacks that go beyond the traditional information und communication technology areas.

[3] "Early detection and mitigation of IT crises", drawn up as part of the KRITIS implementation plan

Botnets Feel the Heat

Willi Herzig, Anti-Botnet Initiative contact person at BSI

The botnet problem has once again worsened significantly over the past two years. We have also seen a rapid increase in professionalized and internet crime with commercial interests. Botnets are being rented out professionally on an international level, and "customers" use them to take revenge or gain competitive advantages, for other criminal purposes like extortion and even for political and religious motives. According to BSI research, users often do not notice that their PC is part of a botnet as it appears to be working normally. An analysis by internet security firm Trend Micro, which looked at 100 million infected IP addresses worldwide, arrived at the same conclusion. It showed that 80 per cent of infected PCs were infected for more than a month, and 50 per cent for more than 300 days. One of the reasons for this is that some bot software can actually deactivate antivirus software to avoid discovery. Often the infection is only discovered when the PC user is alerted to it by their provider.

Launch of Anti-Botnet Initiative

To help someone whose PC is part of a botnet, it is important to inform them about the infection, explain the risks involved, and provide advice and active support for eliminating the malware. The BSI therefore supports the Anti-Botnet Initiative set up by the eco-Association of the German internet Industry to reduce the number of infected PCs. This initiative, which was officially unvei-led on September 15, 2010, aims to make life more secure for the end user and knock the bottom out of botnets operating in or out of Germany for good wherever possible.

As part of the project, participating ISPs inform affected customers that their PC may be infected with a malicious program. They also refer them to the information and tools for scanning and cleaning up the infected PC on the website https://www.botfrei.de. Here users can find in-depth background information, security resources, recommended actions and tools for identifying and uninstalling malicious programs. Users can run the DE-Cleaner to identify and remove malware infections themselves. For stubborn infections, the initiative offers the DE-Cleaner Rescue System CD, which can also be used if the infection cannot be identified on the running system, as is the case with rootkits, for example. This CD was developed in collaboration with COMPUTER BILD magazine and Avira and given away to several hundred thousand users in the magazine's September 2010 issue.

If a user alerted by their ISP needs additional support, they can call the Anti-Botnet Advisory Center support hotline.

BSI Vice President Horst Flätgen (center) at the press conference marking the launch of the Anti-Botnet Initiative (also in the picture: Walter Schumann, Vice President Sales, eleven GmbH (l) and Bernd Becker, CEO, eco IT Service und Beratung GmbH

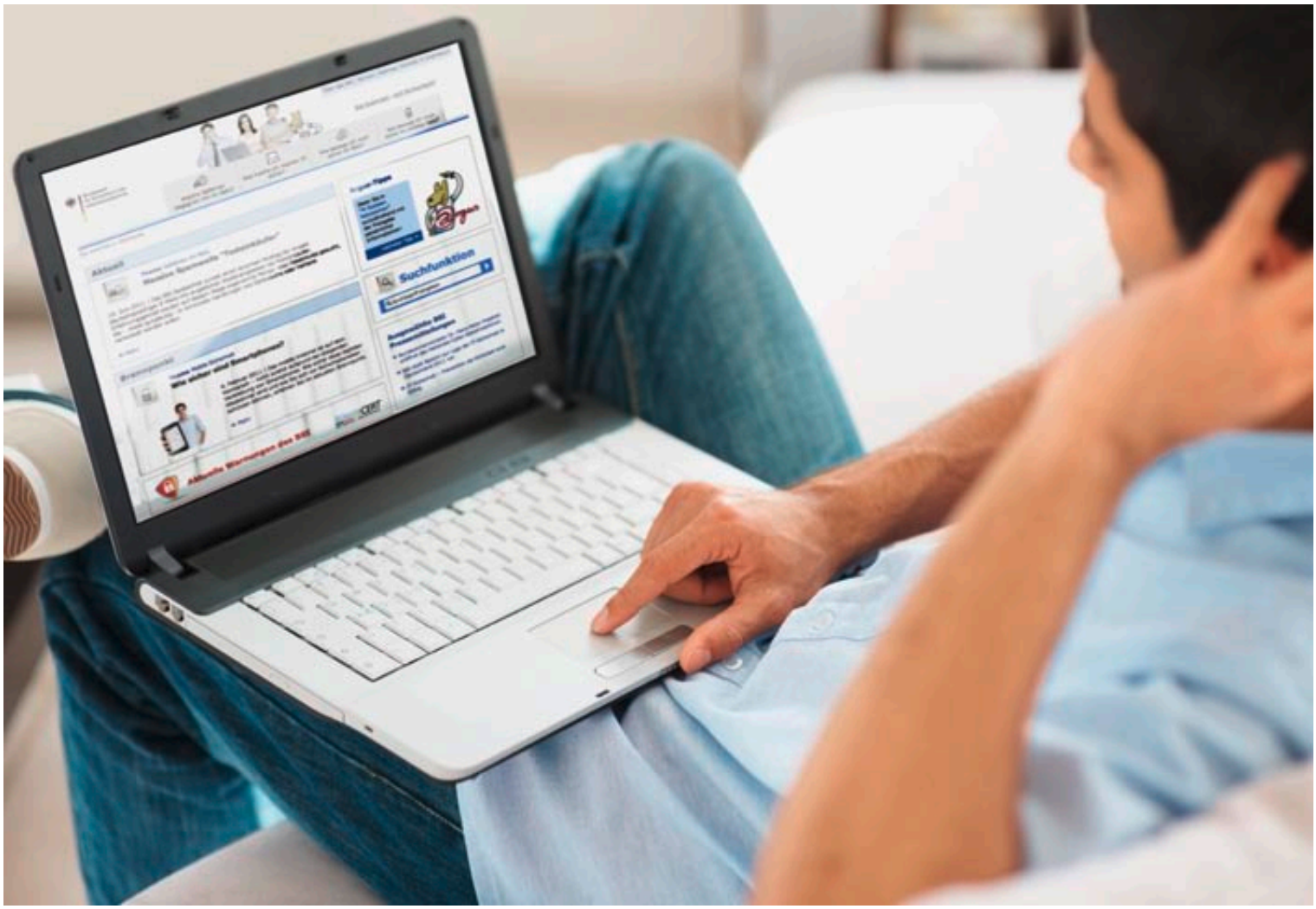
Positive Feedback From Users

The initiative was extremely popular right from the outset, and more partners have since been recruited. Between its launch on September 15, 2010 and the end of the year, more than 710,000 visitors used the facilities on www.botfrei.de. During this time the DE-Cleaner was downloaded and run almost 370,000 times.

In December 2010 the Symantec DE-Cleaner was joined by another one provided specifically for this project by Kaspersky. This new DE-Cleaner is a perfect complement to the existing one, since it can be run offline after downloading. Eco has also recruited more ISPs to the project, who will soon be playing an active role in the Anti-Botnet Advisory Center and alerting their customers to infections. The range of user services has also been extended: the Anti-Botnet Advisory Center website is now also available in English and Turkish.

"In the last two months alone, the Anti-Botnet Advisory Center informed hundreds of thousands of internet users about the dangers of botnets. Together with our partners and with the BSI's support, we can make the internet a good deal more secure for all of us."

Prof. Michael Rotert, Chair, eco-Association of the German internet Industry



Going Online – Securely!

Svenja Schiffer, PR Specialist, BSI

Using the Internet to Raise Public Awareness

IT security is not simply a matter of implementing technical measures. User behavior also plays a key part in ensuring that an IT system is secure. And users can only behave appropriately if they are properly informed about potential security risks and protective measures. For this reason, the BSI not only focuses on technical and organizational aspects of IT security but also works hard to improve awareness and understanding of IT security among private users.

From Theory to Practice

A large number of internet users are still not sufficiently well informed about IT security, as a 2010 representative BSI survey on various aspects of IT and internet security showed. One of the survey's key findings was that there is a yawning gap between the theoretical and practical aspects of internet security for the majority of Germans. For example, between 60 and more than 90 per cent of those interviewed were aware of the risks that can arise when surfing the internet, like viruses, Trojan horses, identity theft, subscription traps, phishing or spyware.

Svenja Schiffer

However, too few people do enough to protect themselves against them. In fact the use of antivirus software has actually fallen since the BSI's 2008 survey. Only 87 per cent of Germans now have antivirus software on their PCs, compared with 92 per cent in 2008. Another example: 63 per cent of respondents surf the net with administrator rights enabled on their PCs, unaware that if the PC is infected with malware, the attacker would be able to take complete control of it.

Communicating With the Public Efficiently

To raise awareness effectively and ensure that the message gets through to the target group, you need to find out what communication channels private users use to keep themselves informed. Our survey revealed that almost half of the respondents find websites the most suitable source of information on IT security. Only one other medium was more popular: PC magazines. This confirms that the BSI is on the right track with its website www.bsi-fuer-buerger.de and is pursuing the right strategy.

The BSI laid the foundation for its public information and awareness raising activities back in 2002, when it launched its Citizens' CD entitled *"Ins Internet – mit Sicherheit!"* (Going Online – Securely!) at CeBIT. To keep pace with the rapid developments in IT security and offer regular information updates, in 2003 we moved from a CD to a website: www.bsi-fuer-buerger.de. This website provides easy-to-understand, technically sound and neutral information on internet threats along with instructions on how to protect against them, along with specific help on selected themes. Private users are also offered contact options via e-mail, phone and fax.

In 2010 we decided to relaunch the website. The main aim of the revamp was to modernize the design, make it more user-friendly and provide more room for topical themes. An intuitive navigation structure guides users through the website. They will find answers to questions like: "What risks could I come across on the internet?" "How can I make my PC secure?" "How can I stay secure on the net?" and "How can I stay secure online on my mobile device?" On the home page users will find information on the topic of the day along with the three latest Bürger-CERT alerts. In a Themes box, BSI-für-Bürger tackles aspects of particular interest and provides updates on specific themes.

With these public offerings, the BSI is specifically addressing a heterogeneous target group so that it can reach as wide an audience as possible. To reach specific audiences, the BSI works with partners who have the same aims but who address different target groups. This collaboration ranges from mutual links on websites and posting BSI information on other websites, right through to sharing information constructively on the latest relevant IT security themes and deciding who will tackle which topic.

By providing these services, the BSI is playing a key role in informing and raising awareness among private users. We fully intend to continue and expand this service going forward in order to reach the ever growing numbers of internet users.

The BSI in the Political and Media Spotlight

Nora Basting, Press Officer, and
Beatrice Feyerbacher, Specialist and Executive Staff Member, BSI

"The many and varied aspects of IT security are earning a permanent place on the media reporting agenda."

Nora Basting

"Many political projects are nowadays also IT projects in which IT security plays a central role."

Beatrice Feyerbacher

Journalists and media professionals regard the BSI for many years as a must-have contact on the subject of IT security. Much of our media liaison work revolves around the BSI's core activities as the federal govern-ment's IT security service provider. But as an independent and neutral body, the BSI also provides hints and information for private users and businesses. Actual topics such as identity theft and phishing, password security and the safe use of social networks are prominent subjects of media inquiries, as well as information security in the corporate environment.

In 2010 the BSI's visibility in the media and public arena once again increased. Besides the ever-growing general awareness of the issues around IT and internet security, this is ascribed to two current developments in particular. Firstly, some large-scale projects in 2010 in which the BSI was involved led to greater public demand for information. The most important milestone in this area was the introduction of the new ID card on November 1, 2010 – a subject that will affect virtually all Germans over the coming years. The BSI had already launched an information campaign in early 2010,

Interview with BSI President Michael Hange

consisting of press conferences, events and stands at exhibitions on the subject of the security architecture of the new ID card and the ways in which it can be used as electronic proof of identity (eID) online.

The BSI was also much in demand for interviews, statements and television reports. Here too, the spotlight was firmly on the security of the data on the new ID card and what the eID function can be used for – not least following critical media reports that gave rise to widespread public calls for clarification.

Secondly, the new authorities given to the BSI in the 2009 BSI Act affect the way the public perceives the BSI. The new law allows the BSI to warn publicly about malware and urgent security vulnerabilities in IT products. The BSI used its new authorities for the first time in January 2010, and throughout the year published a series of bulletins on security vulnerabilities in IT products like operating systems, browsers and other application software. If a widely-used product has a security vulnerability that is at imminent risk of being exploited by IT criminals, the BSI can quickly issue an area-wide alert and recommend steps to mitigate the danger. In such cases, the BSI publishes appropriate advice via the information service Bürger-CERT, together with suggestions as to how people can protect themselves against such attacks.

Numerous other themes were featured on the BSI Press Office's day-to-day agenda in 2010, such as cellphone and smartphone security, and measures against botnets with the help of the Anti-Botnet Advisory Center, an organization set up by the eco-Association of the German internet industry with BSI support. The BSI published more than 85 press releases and memorandums on current issues in 2010 alone. The misceallaneous aspects of IT security are therefore well on their way to attain a constant place on the media coverage.

Politicians are also focusing increasingly on issues regarding IT security, as many political projects are nowadays also IT projects in which IT security plays a central role (e.g. the introduction of Smart Meters). Political awareness has also increased as IT takes on an ever greater significance in our everyday lives and as the ability to act in both the political and economic sphere depends on properly functioning and properly protected IT. These two developments are reflected in the new BSI Act and at the same time the political spotlight shines on the BSI.

The year 2010 was determined by numerous meetings with national and international politicians. Beyond that, the BSI's technical expertise was demanded by various political committees, such as the German Bundestag's Committee on Internal Affairs and the ICT Committee of the Council of Elders. Discussions revolved around a wide range of BSI themes such as the new ID card, security of mobile communication and the BSI Act, of which article 5 (10) imposes on the BSI a permanent duty to report to the Committee on Internal Affairs. In the light of the BSI Act and the new National Cyber Defense Center, political attention will remain focused on the BSI in 2011 as well.

Communicating – Mobile and Protected

IT Security and Mobile Workstations – SINA VW in Practice

Robert Rasten, Project Manager SINA Development, and
Oliver Zendel, Project Manager SINA VW Initiatives, KP II

A project that ticks all the theoretical boxes is only worthwhile if it is given the opportunity to prove its practical value in daily use. Just such an opportunity arose thanks to an initiative in the German government's Economic Stimulus Package II (KP II), in which 14 federal authorities took part. The aim of this initiative was to increase IT security on mobile workstations by deploying BSI-approved components. By using SINA VW laptops, authorities can get hands-on proof that flexible, IT-based mobile working and IT security do not have to be mutually exclusive. Instead, they perfectly enhance each other when modern IT and IT security processes and technology are used.

Pilot Authorities Get First Try

Three pilot authorities were selected to test the implementation of the initiative: the Federal Chancellery, the Federal Agency for Technical Relief (THW), and the BSI. This choice offered broad coverage of different deployment scenarios and enabled a process to be drawn up for implementing the various specific requirements in practice. At each of the pilot authorities the SINA VW (Secure Inter-Network Architecture Virtual Workstation) has been deployed successfully both as a standalone workstation computer and as an additional mobile workstation.

When deployed as a standalone workstation computer, the SINA VW gives its users unparalleled flexibility in terms of where they choose to work without compromising on IT security. It is possible to achieve the status quo of an existing IT setup in an office using a docking station and a permanently installed monitor. But this scenario reveals just how flexible it is when employees can take their workstations with them on business trips or back home for telecommuting, as it maximizes their productivity and ability to work. The SINA VW supports this scenario with approved security functions like VPN Tunnel, hard disk encryption, strong smartcard authentication and encapsulation of individual workstation sessions.

In the second trial setup, the authority has a pool of SINA VWs exclusively for mobile use. This scenario is useful if not every employee can be given a SINA VW, i.e. if there are more users than devices. The aim is to set up a process in which a user is allocated a SINA VW that is adapted to their needs for a specific time. The challenge is to personalize the SINA VW so that the user has all the necessary data and functions they need for their business.

Process for Introducing and Integrating SINA VW

The experience the pilot authorities gained in implementing these scenarios will be shared with future SINA VW users. In line with the concept of avoiding mistakes by learning from others, blueprints for the use of SINA VW are being produced that can benefit other authorities planning to introduce this product. As a result, a process for introducing and integrating SINA VW has been put in place based on the experiences gained by the three pilot authorities. The process can roughly be divided into four phases:

1. Setup of the network and access infrastructure components
2. Adaptation of the workstation operating system to the requirements of a mobile workstation
3. Integration of the SINA VWs into existing operational IT processes
4. Roll-out of devices to users.

SINA VW in Practice

BSI managers have been working exclusively with SINA VW notebooks since mid-2010. The system ensures a high degree of flexibility and a high security level in both stationary and mobile use.

Horst Flätgen, Vice President,
Federal Office for Information Security

The Federal Chancellery needs secure remote access to the internal network for its employees. We are delighted that the BSI has found a solution for this that is available to the whole federal administration.

Dr. Till Nierhoff, Section 114, Federal Chancellery

The Federal Agency for Technical Relief (THW) uses IT for planning, implementing and following up its deployments. At the moment the THW has 54 SINA VWs in active use, which are rated positively by all users.

Angela Huschmann, Section Z5,
Federal Agency for Technical Relief

The BKA has made the use of BSI-certified components a priority. Being able to deploy a product like the SINA VW that meets very high security requirements while retaining full functionality plays a major role in improving IT usage "on the ground". For instance, it enables our officers to use different networks to connect to our central IT on an ad-hoc basis when they are on the road. So they have the police applications they need at their fingertips when they need them. The SINA VW can also be used as a flexible telephone end-device (VoIP softphone) by adding telephone software and a headset. On an existing virtual private network (VPN), officers can now speak to the office securely with VoIP using their usual office telephone functionalities. This is a major step towards secure IT use "on the ground."

Klaus Schiel, IT 06, Bundeskriminalamt

From 2011 German soldiers serving in the ISAF in Afghanistan will be equipped with SINA VW, which will enable them to use different security domains on one end-device for the first time. It will also have the added synergy effect of optimizing network and system administration.

Colonel (GS) Armin Fleischmann, IT-AmtBw

It turned out that most time and effort had to be focused on adapting the workstation operating system to the requirements of a mobile workstation. This is not surprising, since most of the federal administration's workstation operating systems are not designed for mobile use. To ensure that the low bandwidths and high latencies in mobile connectivity do not affect the system, it is often necessary to adapt and optimize the workstation operating system in a specific way. However, these are worthwhile investments in the authority's IT infrastructure, since they not only make the workstations suitable for mobile use, but they generally also result in optimizations on non-mobile workstations.

By mid-June 2010, the process of introducing SINA VW was sufficiently well-established for other authorities to be equipped with these devices as part of this initiative. In this second wave, the foundation was laid for the use of SINA VW at eleven authorities.

SINA VW at the BSI

The SINA VW pilot installation at the BSI was a particularly important one. For one thing, it is a sign of credibility that the authority that is responsible for the system is using it in large numbers. For another thing, the use of the system by the BSI enables valuable conclusions to be drawn in terms of the next stages of the development.

More than 70 BSI employees are already using the SINA VW as their sole workstation for their daily business. It is particularly worth mentioning that the BSI's management, including the department head, switched to using the SINA VW exclusively at an early stage. By selecting different types of users, it was possible to prove that the SINA VW can be used at all levels of an organization and that it delivers the necessary measure of IT security for the tasks concerned.

Tried and Tested in Practice

So far 700 SINA Virtual Workstations have been set up in the federal administration. In addition, blueprints have been developed that make it easier for authorities to integrate SINA VW-based mobile workstations into their IT infrastructure. The initiative has impressively demonstrated that a ready-to-use product for the mobile workstation scenario is already available. This product – the SINA VW – consistently and reliably combines the flexibility of mobile working with the need to adequately protect sensitive information. The experience the various authorities gained during the introduction in areas such as device management will be used to take the project to the next level. Following the success of the introduction of the SINA VW in the federal administration, it was decided to extend the initiative by a further year and provide additional SINA VWs for the federal administration.

We need a high security level for mobile working as well.

Mobile and Secure With the BSI:

Solutions for Optimizing Secure Communication on Smartphones in the Federal Administration

Joachim Opfer, Head of Counter-Eavesdropping, BSI, and Marion Brinkkötter, SNS Project Team Member, BSI

Being able to access information on the move with smartphones is a major success factor in all areas of business these days – from the public sector to industry, banks and insurance companies. Smartphones have therefore become an indispensable tool in our everyday working lives. So reliable availability and the security of personal and confidential information are becoming increasingly important.

Nonetheless, mobile communication with smartphones is potentially very high-risk. Smartphones are usually operated in an insecure environment, with the result that the data stored on them (emails, SMS, calendars, contacts, files) can easily get into the wrong hands if the device is lost or stolen. In addition, wireless communication via public mobile networks is particularly easy to intercept. The mobile communication standard provides for encryption of information transferred across the airwaves, but it has weaknesses that are relatively easy to exploit. For this reason, the standard encryption provided on mobile networks is inadequate for protecting the federal administration's highly sensitive data.

IT Investment Program: More Products Deliver Better Mobile Security

At the beginning of 2009, the federal government approved the IT investment program as part of the Pact for Employment and Stability in Germany. As part of this measure, the federal administration procured a number of secure mobile voice and data communication products that factor in security and meet the BSI's security requirements. The BMI (Federal Ministry of the Interior) and the BSI are responsible for this initiative, and the BSI is tasked with its implementation.

"The standard encryption provided on mobile networks is inadequate to protect the federal administration's sensitive data."

Joachim Opfer

SiMKo2 Enables Secure Data Exchange with Mobile Handsets

The SiMKo2 system produced by T-Systems was selected for secure mobile e-mail and PIM[4] communication. This product is the only one on the market that is recommended specifically for use with classified information up to classification level VS-NfD (Classified Information – Restricted). Because it uses Virtual Private Network (VPN) technology, SiMKo2 enables e-mails and PIM data to be exchanged securely between mobile handsets (PDAs) and an enterprise server. All the data stored on the handset are encrypted. Authentication is certificate-based, using the federal administration's Public Key Infrastructure (V-PKI). Initial demand among the highest federal authorities and security services was set at 4,000 handsets across 30 authorities. During 2010 the existing IT infrastructure was upgraded and adapted step by step for the use of SiMKo2. It was important to continue to meet the future users' specific needs and background requirements, such as high availability, virtualization and replacement or integration of existing firewalls. To keep pace with the short product cycles in the smartphone market and the users' desire to have the very latest handsets, standard commercial smartphones are constantly being adapted for secure use in the SiMKo2 system. Every new type of SiMKo2 handset is subjected to a security evaluation and approved for compliance with the security standards by means of a BSI endorsement. The smartphones currently endorsed by the BSI are the HTC Touch HD, the HTC Snap and the HTC Touch Pro2. Other handsets will follow as new smartphones are introduced. SiMKo2 is also suitable for voice and SMS communication, although at the moment no additional encryption is available for these. The next challenge will be to develop a component for voice and SMS encryption on SiMKo handsets that complies with the BSI's Secure Trans-Network Voice Communication standard (SNS).

SNS – BSI Secure Trans-Network Voice Communication Standard

There are various end-to-end encryption systems that protect against sophisticated eavesdropping attacks on mobile voice com-munications and SMS messages that use systems like IMSI Catcher[5] and Rainbow Tables. This hardware or software, which is usually manufacturer-specific, protects the information being transferred between mobile handsets against third-party access. However, there is no interoperability between different manufacturers' systems. In fact, users of these encrypted cell phones can only set up secure connections to other handsets from the same manufacturer, with the result that these systems have so far been very limited in terms of usability and practicability. The answer was to come up with a manufacturer-independent standard. The BSI developed just such an interoperability standard in 2010 as part of the IT investment program and in cooperation with manufacturers including Rohde & Schwarz SIT, Secusmart and T-Systems.

The declared aim of this Secure Trans-Network Voice Communication Standard (SNS) is: to implement and define the "secure telephony" and "secure SMS" functions such that:

- interoperability between manufacturers is guaranteed,
- manufacturer-specific solutions are also supported,
- different communication connections and networks can be used and
- the VS-NfD security level is achieved.

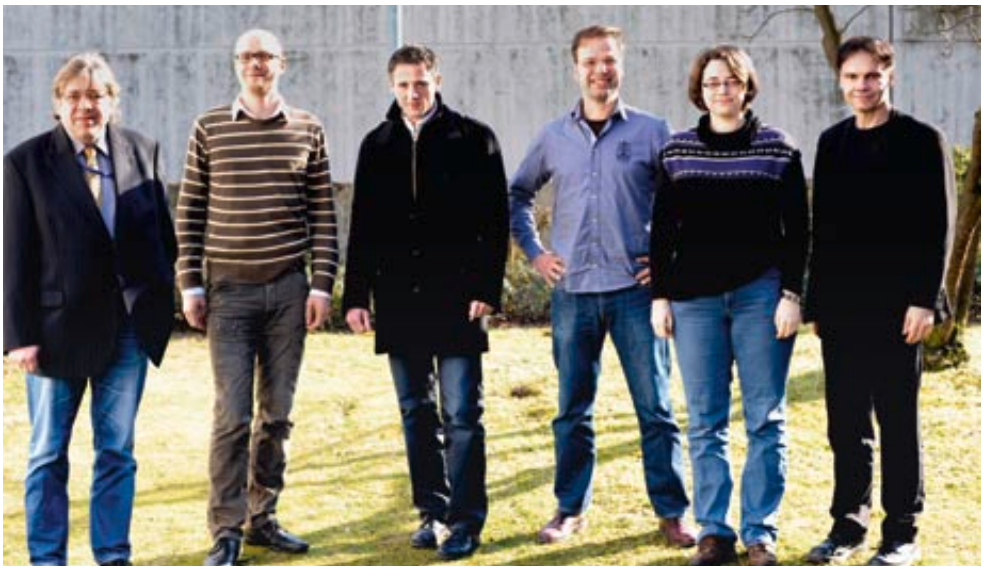
Furthermore, the federal administration should be equipped with handsets that support this standard.

5,600 SNS Standard Handsets Already in Use

The first version of the SNS standard was completed in March 2010 and has been available to all interested manufacturers ever since. Rohde & Schwarz SIT and Secusmart started building the first SNS-compliant handsets over the following months, and by the end of the year the federal administration had taken delivery of 5,600 of these new devices.

New Development: Landline Network Also SNS-ready from 2011

Users should not be entirely dependent on cell phones for secure voice communication, however, but should also be able to take SNS calls on their office landlines. So work is already under way to develop SNS-ready landline receivers, which will be on the federal administration's desks by the end of 2011. The prototype TETRA[6] ◄► PSTN[7] Gateway, also currently under development, will be a gateway between the telephone network and the new digital BOS[8] police radio network. It will allow for secure telephony between TETRA radio handsets and secure cell phones.



The BSI's SNS Team: Dr. Frank Niedermeyer, Dr. Sören Werth, Christian Schridde, Matthias Hirsch, Marion Brinkkötter, Dr. Antonius Klingler (from left to right).

Seamless Integration with Other Networks

The Secure Trans-Network Voice Communication standard was designed to be channel- and network-independent. At the moment, the GSM network data service and the ISDN data channel for landlines are used for mobile communication.

When a connection is set up, the terminals negotiate an operating mode without the user's involvement. This sets the technical parameters for the ensuing call. To ensure interoperability in every case, the SNS standard has two operating modes that must be supported by all approved terminals:

- Operating mode 1 was defined on the basis of the encryption process developed for the TETRA standard. With the support of a gateway, it enables secure communication between BOS radio handsets and SNS encrypted cell phones.
- Operating mode 2 is intended for telephone calls on the PSTN network and can use the whole of the available bandwidth, achieving better voice quality.

Advantage: Standard Allows for Additions

The standard allows other modes to be added. This has the advantage that manufacturers can retain their own concepts and offer their customers enhancements such as more features or better voice quality. The BOS crypto-chip was selected as a security anchor for the standard's two operating modes. It protects particularly security-critical codes and encryption functions against viruses and other malware. The BSI originally developed the chip for the new digital network for authorities and organizations with security functions (the BOS network).

The use of the crypto chip enables interoperability with the end-to-end encryption system on the BOS network. It can be licensed by manufacturers for use in their products. The call key is agreed individually at the beginning of the call using a Diffie-Hellman protocol. User authenticity is ensured using PKI and is verified when the connection is set up. The certificate is saved on the card. For voice communication, the SNS standard currently only supports full duplex telephone calls. However, measures have been put in place to enable the standard to be extended at a later date to include conventional radio operation, i.e. group communication. This will enable it to be seamlessly integrated into the BOS network. To exchange secure SMSs, the handsets agree keys during the voice communication without any user intervention or loss of voice quality. These keys are saved in encrypted form and changed automatically. Encrypted short messages can also be sent between the telephone network and the BOS network.

"The Secure Trans-Network Voice Communication standard was designed to be channel- and network-independent."

Marion Brinkkötter

[4] PIM: Personal Information Manager
[5] IMSI catchers simulate a base station so that the attacker can intercept the victim's call with a man-in-the-middle attack. For more information, please see the brochure *Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte* (PDF, in German only) and the BSI's security information.
[6] TETRA: Terrestrial Trunked Radio
[7] PSTN: Public Switched Telephone Network
[8] BOS: authorities and organizations with security roles

Secure Electronic Identities

The New ID Card:

Technical Concepts for Enhanced Functionality

Bernd Kowalski, Head of Department, BSI

The New ID Card

In the new ID card (nPA) introduced in November 2010, German citizens have more than just a new credit-card format photo identity document. This card also has various electronic functions that greatly improve security on the Internet, including eID, an online ID function that people can use to prove their identity online beyond doubt. A radio frequency chip (RF chip) embedded in the card contains all the information that is displayed visually on the document. In addition, the Qualified Electronic Signature function enables the user to sign documents and declarations of intent online in a legally binding way. Unlike the online ID function, this feature requires the user to purchase a certificate and load it onto their ID chip.

Benefit for the Citizen:
Better Security for Personal Data
In addition to the online ID and signature functions, the new ID card's RF chip also carries biometric data. This provides a stronger link between the card holder and the document, and enables it to be uniquely assigned to the holder. The biometric data can only be read by an authority authorized to establish the person's identity, such as in police, border or customs checks. The card gives access not only to personal details but also to a photograph and fingerprints, the latter being a voluntary feature.

"The electronic functions of the new ID card offer plenty of scope for redesigning access to e-business or e-Government services."

Bernd Kowalski

The project, which the BSI was intensively involved in for a number of years and will continue to work on in the future, reached an interim high point with the introduction of the new ID card on November 1, 2010. Initial thoughts on a digital ID card, as it was known then, were discussed as early as 2002. The BSI was involved in its design even at that early stage. The ID card's central properties such as strong access control and mutual authentication were defined based on technical concepts developed by the BSI.

BSI Ensures Technical Quality

The BSI established the security standards in preparation for the introduction of the new ID card in 2010, and also guarantees the quality of the technical processes that enable the card to be used on the Internet by updating and maintaining these standards. The chip itself and the devices and programs used with it are certified by the BSI. To obtain BSI certification, they

Following the success of the tests, private companies and public authorities are starting to offer applications using the online ID and signature functions.

must meet certain IT security requirements in accordance with the BSI's Technical Guidelines and Protection Profiles. Besides data security, the aim of these is to ensure interoperability between all components. Technical testing is performed by test centers authorized by the BSI.

The production of the specifications was followed seamlessly by support for the public bodies and private companies involved in the implementation, ranging from technical pilots to the field test in which the municipalities were connected, and the application tests for integrating the service providers' applications.

New Opportunities to Shape Business Processes

The electronic functions of the new ID card offer plenty of scope for redesigning access to e-business or e-Government services. In the practical tests, in 2009 and 2010 well in excess of 200 companies and authorities tested the new online ID card and signature function and integrated it into their business processes on a trial basis. The main aim of these tests was to check the practicability, usability and acceptance of the new electronic ID card. Following the success of the tests and the introduction of the new ID card, private companies and public authorities are starting to offer applications using the online ID and signature functions.

The AusweisApp – Successful Implemen-tation Despite Teething Problems

To use the online ID function, the cardholder needs client software such as the free AusweisApp and a contactless card reader that they connect to their PC. The function enables the cardholder and the service provider to prove their identity beyond doubt, and secure communication between citizens and private or public sector organizations on the Internet is significantly simplified.

Shortly after its launch in November 2010, the BSI had to withdraw the AusweisApp briefly because of a security vulnerability that occurred despite extensive preparatory testing by a great many well-known companies, and a revised version of the software was issued a little later. The security of the nPA and the protected data stored on it were not affected by the security vulnerability. Nevertheless, the BSI subjected the processes around the update procedure to thorough testing in order to evaluate problems with the AusweisApp reported by users and service providers as soon as possible and provide the necessary updates promptly. In future, accumulated updates will be issued to add improvements to the card's functionality, user-friendliness and performance.

Improved Data Security

Particularly in the light of the ongoing high risk situation, the electronic functions of the new ID card are a step in the direction of improved data security. The data stored on the card's chip are encrypted by secure cryptographic protocols during transmission. The same applies to the communication partner (public authority, private company) during the mutual authentication process: its data are also transmitted encrypted. The cardholder has full user control of his or her data at all times with the double security measure of possession and knowledge, provided he or she does not surrender possession of the ID card or reveal the PIN.

The nPA in Practice

DATEV eG is a Nuremberg-based software company providing IT services for tax consultants, auditors, and lawyers and their clients. DATEV integrates the eID function into an employee portal to ensure secure online access to documents such as pay slips. Employees can only log onto this employee portal by proving their identity electronically using the new ID card. The company started by posting the pay slips of around 700 DATEV employees on the portal. Participants can view their pay slips online, download them and print them out. DATEV plans to offer these and other employment-related cloud services as a general service for tax consultants and employers.

"Since using secure DATEV IT SERVICES, DATEV members and their clients have become familiar with the principle of 'Possession and Knowledge'. The nPA will complement DATEV-myIDentity and DATEV-SmartCard and will therefore facilitate online services for employees. In the nPA concept, we believe that it is important for the providers to prove their identity to the user by means of an authentication certificate first, and to tell the user what data on the nPA they are permitted to read in a particular usage scenario. This engenders trust on the part of the user and enables the service provider to guarantee compliance with central data protection requirements."

Prof. Dieter Kempf, Vorstandsvorsitzender DATEV eG

The New ID Card – a Showcase Project For Germany

Fujitsu is the first company to integrate the new ID card in its e-commerce platform. Since November 2010, nPA holders in Germany have been able to order products from the German Fujitsu Online Shop and track their orders using the new document. The nPA's online ID function is integrated directly into Fujitsu's online ordering process. This enables the legal capacity and the identity of a buyer to be quickly established without infringing data protection laws. The customer in turn benefits from faster and more convenient ordering processes.

"The new ID card is a world first – and we at Fujitsu are proud to be one of the first companies to use it. Users can already register with the new ID card in Fujitsu's online shop. But it is not just consumers who benefit from the technology: it also helps private and public sector organizations make their business processes more efficient, and make their online services easier to use, more secure and therefore more customer-friendly."

Rolf Schwirz, CEO Fujitsu Technology Solutions.

The New German ID Card in the European Environment

Dr. Andre Braunmandl, BSI Project Manager, STORK eID-LSP

In the age of electronic business processes, large online platforms for trading, auctions, information gathering, and leisure activities, the issues of data protection, the reliability of online services and the security of online transactions are of central importance. The new German ID card's electronic functions developed by the BSI play an important part in this with their secure, trustworthy electronic authentication function (online ID, or eID).

To enable German citizens to use the benefits of the new ID card for internet services right across Europe, the BSI is actively involved in the European Union's eID interoperability program. With a view to achieving synergies in the use of the Member States' electronic authentication functions right across Europe, the European Commission set up a Large-Scale Pilot (LSP) project entitled STORK (Secure Identity Across Borders Linked). From 2008 to 2011, this project has been bringing together European activities around the interoperable use of electronic identities. The STORK Consortium originally consisted of 29 partners from 14 Member States. At the beginning of 2010 it gained three additional Member States that had previously not participated. The BSI was extensively involved in STORK right from the beginning, and will incorporate the results of the project into the ongoing development of the German eID infrastructure.

For Europe, interoperability of national eID solutions is a major step towards harmonization. It plays a key role in enabling EU citizens to use many cross-border e-Government services, such as those described in the Services Directive. The tool of the Large-Scale Pilot (LSP) is particularly promising in this area because it brings together all the key players in eID solutions from the various EU Member States.

A European Approach to Interoperability

The eID infrastructure of the new German ID card meets the high European data protection and security requirements for the first time. It is therefore eminently suitable for achieving the European Commission's vision of a pan-European e-Government structure. The model for bringing about interoperability between European eID systems developed in the STORK eID LSP is designed to link the various national systems via national Pan-European Proxy Services (PEPS). The German model allows direct communication between service providers and holders of the new German nPA ID card. Against this backdrop, the BSI is tasked with laying the foundation for enabling European service providers' authentication certificates to be stored securely in the PEPS and for ensuring that only the authenticated service provider can gain access to the personal data of the cardholder via this authentication certificate. To achieve this at a European level, the service providers must be connected to their national PEPS with a secure, reliably authenticated connection.

Working with industrial partners, the BSI has developed a solution that is to be piloted as part of STORK in 2011. A European interoperable solution is therefore within reach.

And Post-STORK?

SECURE IDENTITY ACROSS BORDERS LINKED

Connecting national eID systems via PEPS only solves part of the current interoperability problem. From the point of view of mobility, the problem remains that EU citizens wanting to authenticate themselves using their eID token when traveling to other Member States would have to carry the necessary hardware and software with them. Obviously this is impractical. To establish eID as the basic technology in Europe on which cross-border applications can be developed, the European Commission is planning to further develop the interoperability of eID post-STORK. All stakeholders agree that eID interoperability is an infrastructural factor that plays a significant part in the competitiveness of the modern European economy. The BSI is committed to continuing its active involvement in these developments and therefore acting as a driving force in Europe.

"T-Systems has been working closely with the BSI for many years, and thanks to this relationship we have been able to work with the BSI on the STORK project since its inception. T-Systems coordinates a group of German industrial partners in the project. Our shared aim is to uphold and roll out the high German security standards for the harmonization we are aiming for or, in more concrete terms, the interoperability of the various national eID solutions. Based on the close relationship of trust we have developed with the BSI, Germany can play a key role in the STORK project, which is reflected specifically in the first application pilots led by the German participants. Besides the governmental applications demonstrated nationally in the application test and internationally in the STORK pilots, the commitment of the BSI and its intensive cooperation with German industry are enabling us to build up an eID infrastructure that will also be able to be used for commercial purposes."

Volker Reible, Vice President Large Scale Project Management, T-Systems International GmbH

Tackling the Challenges Together

"In the Age of Internet, No Country is an Island."

Four questions for Neelie Kroes, Vice-President of the European Commission and Digital Agenda Commissioner

In 2010 the European Commission adopted the Digital Agenda, which is Europe's strategy for a flourishing digital economy by 2020. As trust and security are crucial to this endeavor, what are the most important measures for the EU to strengthen network and information security?

The Digital Agenda for Europe (DAE) is one of the flagship initiatives under the Europe 2020 Strategy. It reflects our vision on the efforts we need to make in the next few years to fully embrace the digital society. It clearly identifies trust and security in the online world as key contributors to a vibrant digital society and to smart, sustainable and inclusive growth. In the trust and security pillar of the DAE, we define 14 action points that aim at improving Europe's capability to prevent, detect and respond to network and information security (NIS) problems and to fight cybercrime. Some address data protection issues, awareness raising measures and child protection in a safer internet environment. Coordination at EU level and the tasks of Member States as well as areas for cooperation on a global scale are also mentioned. Among the key priorities I would highlight the cooperation of Computer Emergency Response Teams (CERTs) and fostering the multi-stakeholder dialogue between public and private sector.

Let me give you a couple of examples of what we have already accomplished. On September 30, 2010, the Commission presented to the European Parliament and the Council of Ministers a proposal for a regulation modernizing and reinforcing ENISA, the European Network and Information Security Agency. On the same day, the Commission also tabled a proposal for a directive on attacks against information systems to deal with new cyber crimes, such as large-scale cyber attacks. This was followed by the first pan-European cyber-security preparedness exercise on November 4, 2010, called "Cyber Europe 2010", which took place with the participation of all Member States and the support of ENISA and the EU Joint Research Centre.

Cyber attacks in particular are growing in sophistication and frequency. What are the Member States' and the European Union's roles and responsibilities in protecting Europe?

Addressing cyber threats and strengthening security in the digital society is a shared responsibility – of individuals as much as of private and public bodies, both at home and globally. Member States are primarily responsible for national cyber security strategies and

their implementation. However, the security of each Member State depends also on the cyber security level in other Member States. The collective aim should be to achieve a high level of NIS throughout Europe and to overcome the existing significant differences between Member States in terms of preparedness and capabilities. Let's keep in mind that we are all interconnected and that a chain is only as strong as its weakest element. In the age of Internet, no country is an island – and I am glad to see that this has been very well understood in Germany. The EU, notably through ENISA, also plays its role in this very dynamic environment. Firstly, we support Member States in their efforts to improve their cyber security capabilities. Secondly, we promote and support cooperation between Member States and the private sector on prevention, preparedness and response. Thirdly, we strive to create a level playing field for NIS in Europe to ensure that industry and businesses find their way in the diversity of security requirements and practices.

Which leads to the question, what could be the role of Germany and its cyber security authority BSI to help in this European context?

Germany is very advanced in many respects and does an excellent job in promoting European cooperation on cyber security. This is particularly true in the technical area, where the BSI's activities and projects make a valuable contribution to develop European know-how. We appreciate, for instance, the fact that the BSI has given a helping hand to new Member States to establish their governmental CERTs. In the future, I would like to encourage Germany, together with those Member States that have advanced capabilities, to share their knowledge on cyber security preparedness. In this regard, the German National Cyber Defense Center and the German Anti-Botnet Initiative are good examples which have the potential to deliver benefits throughout the EU.

What especially interests us: what are your initiatives to promote good security practices within the Commission and across other European institutions?

I am a firm believer that we must always practice what we preach. Firstly, the European Commission is determined to adopt internally, as an organization, the best available standards and practices for security, of which NIS is a core component. Secondly, I have launched in the DAE the idea of establishing a CERT for the EU institutions. Such a CERT would be crucial in enhancing the security of the EU institutions and make it comparable to the highest standards at national and international level. In this regard Vice-President Šefčovič and I have established a high-level expert group, the *"Rat der IT-Weisen"*, to advise the European Institutions on how to set it up. The experts delivered their report at the end of 2010. We are now engaging with other EU institutions on the way forward. My objective is that, by 2012, the community of governmental/national CERTs will have someone to call in Brussels should they detect a cyber-attack against our organizations!

Digital Agenda – a Political Flagship Initiative for Growth and Well-Being in Europe's Information Society

Neelie Kroes, European Commissioner for the Digital Agenda, published the Commission's eponymous political umbrella strategy in a communication on May 19, 2010. This is the first of seven flagship initiatives of the Europe 2020 strategy.

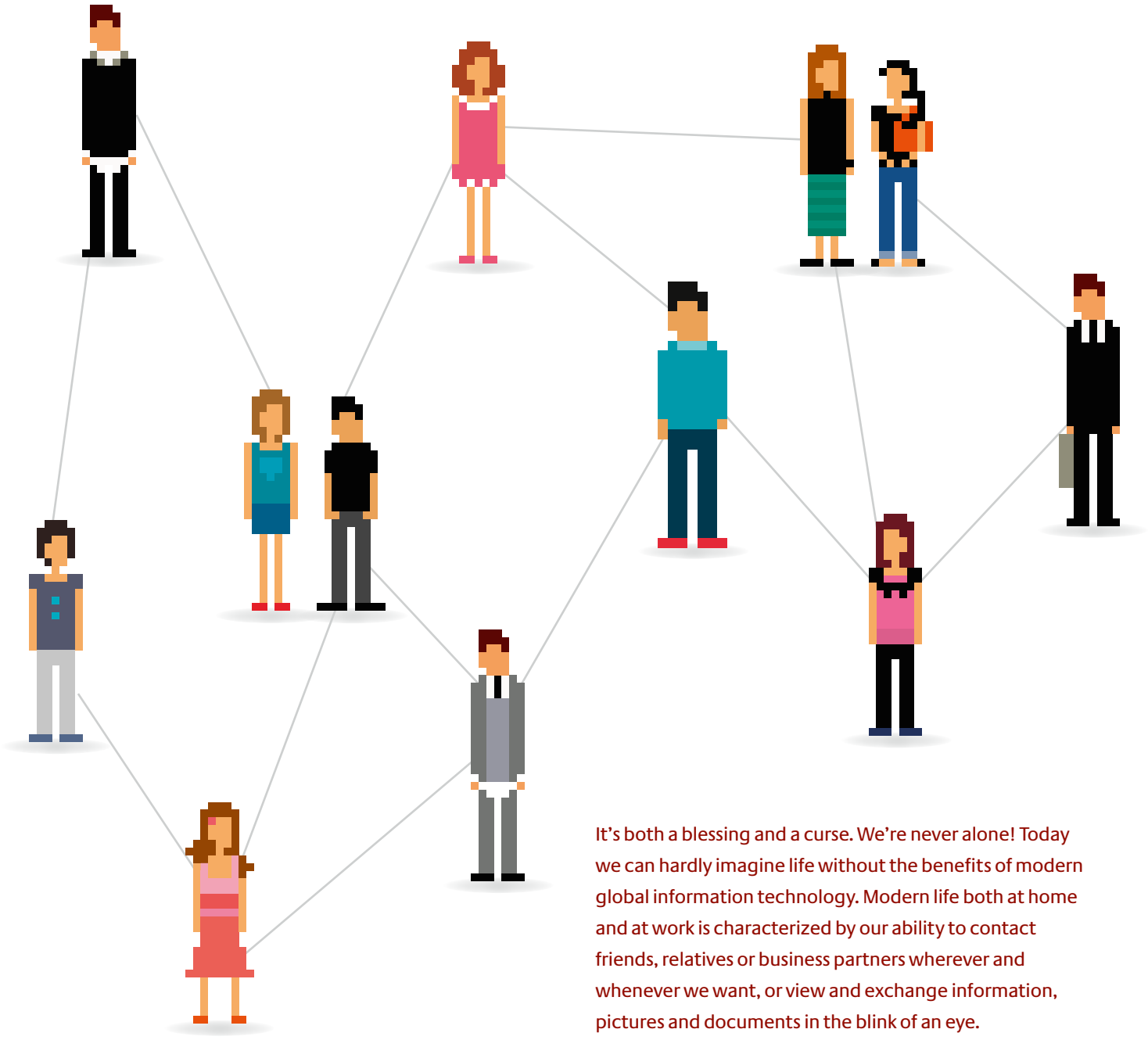
It was set up to define the key enabling role that the use of information and communication technologies (ICT) will have to play if Europe wants to create growth and prosperity. It is therefore a strong reflection of the opportunities for growth in the digital age. The Digital Agenda provides for some 100 follow-up actions, of which 31 would be legislative.

The seven key action areas, or pillars, are:

1. Creating a digital single market
2. Improving ICT standards and interoperability
3. Improving trust and security on the Internet
4. Better access for Europeans to fast Internet
5. Increasing advanced research and innovation in ICT
6. Enhancing digital literacy, skills and inclusion
7. ICT-enabled benefits for EU society

Global Information Technology – International Cooperation

Hans-Peter Jedlicka, Planning and International Cooperation Specialist, CERT-Bund



It's both a blessing and a curse. We're never alone! Today we can hardly imagine life without the benefits of modern global information technology. Modern life both at home and at work is characterized by our ability to contact friends, relatives or business partners wherever and whenever we want, or view and exchange information, pictures and documents in the blink of an eye.

Benefits That No-one Wants To Be Without

The omnipresence of information technology, the ability to constantly achieve rewarding goals, and the availability of valuable information stored or transmitted via IT also have the downside of attracting people intent on abusing this selfsame IT for their own purposes. Hardly a day goes by without a new malicious program being spread or important data stolen, be it personal data, customer data, credit card information, login credentials or similar. The perpetrators are protected by the anonymity of the internet and deliberately use the options offered by IT to conceal their own identity and make it harder for the authorities to take effective measures, including prosecution.

There is an incessant barrage of compromise attempts aimed at further expanding the networks of infected and controlled systems, or botnets. Even respectable websites are being attacked and manipulated so that the unsuspecting and unprepared user downloads more than just the content they were looking for: they end up with a malicious program installed on their system as well. From then on, the compromised system is controlled remotely by the attackers, who will also often monitor the user's browsing behavior or mine their personal information.

It is the very transparency of our online behavior and the availability of our data – in other words, the main advantages of our information age – that become distinct disadvantages when seen from this angle.

We're Never Alone Out There

This sobering realization requires everyone concerned, particularly those with responsibility for the security of information and systems, to rethink the way we behave. But users too need to be made aware of the real threats that exist out there and how they can protect themselves effectively. Manufacturers strive towards ever higher quality standards, do all they can to avoid errors and vulnerabilities, and put processes in place to eliminate any security problems that do arise as quickly as possible. The bodies responsible for IT operations and IT security agonize over pragmatic solutions to combine the functionality of necessary applications and their efficiency and user-friendliness on the one hand, and the essential security aspects on the other. Despite much success to date, all stakeholders will need to make a lot more effort, not only to maintain the status quo in the long term but also to make a tangible difference to the situation.

National and International Cooperation

Computer Emergency Response Team (CERT®)
The idea for the Computer Emergency Response Team dates back to 1988, when the Morris worm caused significant damage to large parts of the then manageable internet.
To be better equipped to handle future incidents, the Defense Advanced Research Projects Agency (DARPA) initiated the eponymous CERT Coordination Center at Carnegie Mellon University.
Synonyms:

CSIRT	Computer Security Incident Response Team
CIRC	Computer Incident Response Capability

A key aspect of IT security is the regular exchange of information and experience and mutual support within national and international organizations dedicated to security in information technology. At an operational level, this includes the Computer Emergency Response Team (CERT) and manufacturers', businesses' and authorities' own security teams. The benefits of close, intensive cooperation between these bodies has long

been apparent. Cooperation models and relationships of trust have been developed over time that play a significant role in defusing the general threat situation and identifying new risks at an early stage. Analyses are conducted, situation evaluations are exchanged and joint mitigation measures are developed.

Successful German Initiative

Germany is home to one of the world's most closely knit networks of CERTs, known as CERT-Verbund. This consists of several dozens of teams from public authorities, industry and academia. Regular contact, constant dialog and joint projects boost the team spirit and enable what are initially relatively fragile relationships of trust to constantly be strengthened and developed, so that ultimately even sensitive issues can be discussed openly. This community faced a particularly tough endurance test last year in the form of Stuxnet. This ultimately proved to be an opportunity, however, and impressively demonstrated how quickly and efficiently the community was able to work together and pass on information.

We know from experience that incidents soon reach the ears of others, even if one would rather keep them quiet: either their systems are compromised directly, causing actual damage, or attacks are registered and discovered when they are evaluated. Staying mum helps no-one. The only way to ensure that you fully understand your own security vulnerabilities and can protect yourself against further damage is to exchange information quickly and on a basis of mutual trust. Our excellent working relationship with the BSI, or specifically CERT-Bund, has enabled us to safeguard this information exchange for key national networks.

Dr. Klaus-Peter Kossakowski, CEO, DFN-CERT

IT Events Do Not Respect National Borders

This extremely positive experience gained in educating the public about Stuxnet proved to be the case in the international arena as well. The expertise of a wide range of teams enhanced the emerging picture of the overall situation and helped those involved assess it. Quite independently of the highly effective media event that was Stuxnet, the international cooperation that has taken place over the past few years has time and again proved itself to be highly efficient within the resources available. Working closely with the relevant national competent authorities and contact points, we were able to identify, purge or remove from the internet a series of attacked IT systems that were outside of our own jurisdiction. Two aspects in particular call for joint international cooperation to ensure that we can continue to take action: firstly, the increasing tendency to use powerful, multifunctional botnets that are generally distributed worldwide for abusive purposes, and secondly, the growth in specialization and task sharing among the perpetrators, who are also often organized on a worldwide basis. Automated malware distribution routines do not, after all, respect national borders or legal systems. On the contrary, some perpetrators deliberately exploit the complexity of different jurisdictions and factor in potential conflicts of interest when their attacks are brought to public attention, tracked down and removed.

"Over the course of the years we here at CERT-FI have learned that victims of many internet threats are among the last ones to learn about the information security incidents affecting them. CSIRTs play an important role in matching information about incidents with those with a need-to-know. CERT-FI would not be able to succeed in protecting Finland without the continued help of competent and trusted international colleagues such as CERT-Bund of Germany."

Erka Koivunen, Head of CERT-FI, Finland

Who Can I Turn to for Help?

From the point of view of the BSI and the federal government's Computer Emergency Response Team, CERT-Bund, 2010 was marked in particular by their successful efforts to revitalize contacts with national and international cooperation partners, build new relationships, formalize existing processes and work out and rehearse Standard Operating Procedures (SOPs). For example, in addition to the widely publicized CYBER EUROPE 2010 exercise, several other exercises were performed with different groups of participants with a view to deepening relationships and optimizing the response processes.

"We can only move forward together successfully if we know we have reliable partners by our side all the time."

Hans-Peter Jedlicka

Luckily We're Not Alone

All our past experience points to the need for focused cooperation based on trust. An admission that an IT incident has taken place or even the passing on of details about such an incident is often accompanied by the questions: "Do I want to discuss it with anyone else?" or "Should anyone else even get to hear about it?". But in many cases it is only this active exchange of information that enables the relevant competent authorities to take action. Overcoming this reticence is therefore the declared aim of the BSI's cooperation efforts. We can only move forward together successfully if we know that we have reliable partners standing shoulder to shoulder with us all the time.

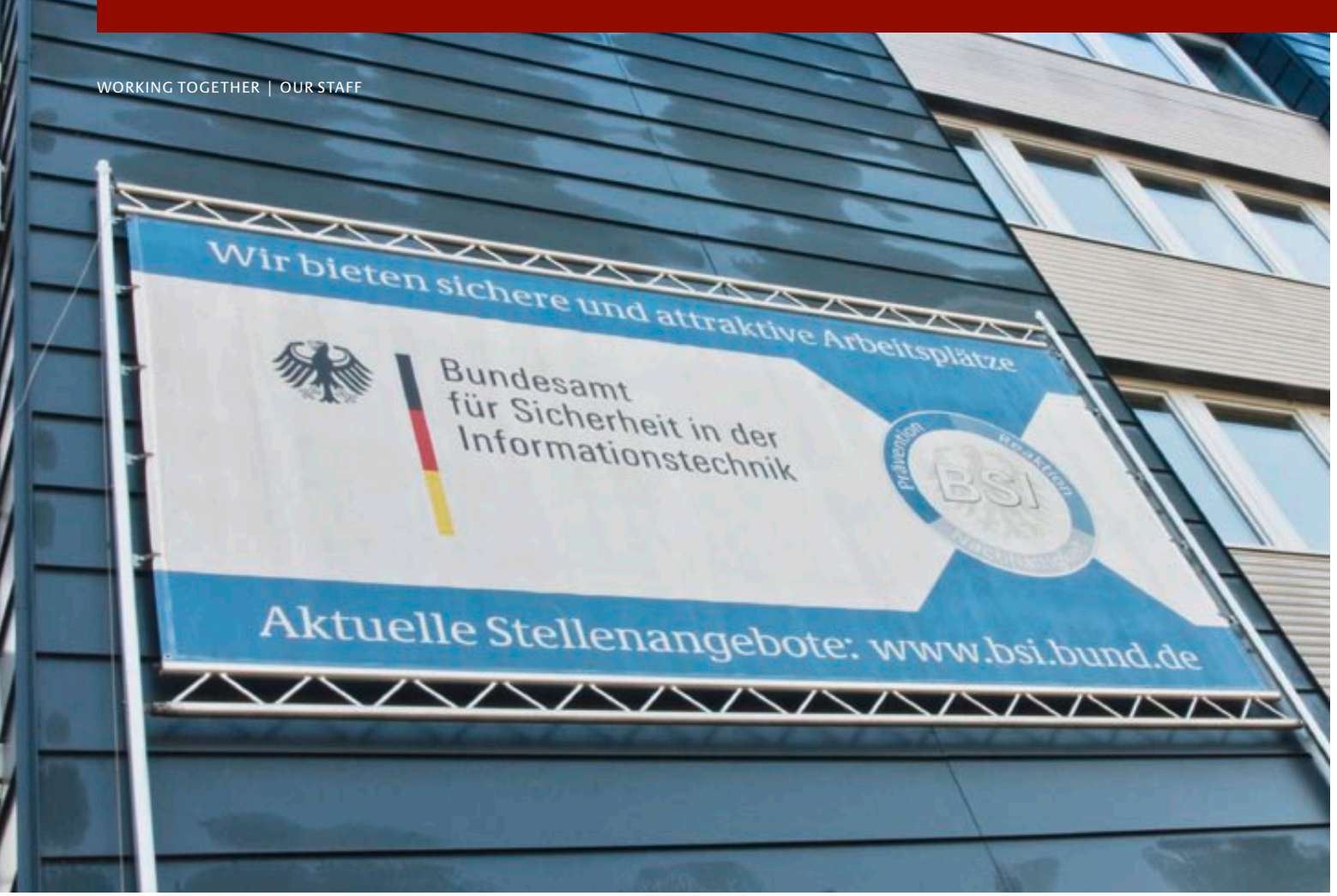
The Secret to Success: Reciprocity

A dominant feature of the successful cooperation models supported by the BSI is the fact that those concerned are closed groups of a manageable size who can rely on the fact that their internal communications are protected and respected. The members generally pursue identical goals and share a common understanding of each other.

Based on the commonalities, processes and procedures are developed that help make communication in and response to IT situations and crises more efficient. Regular meetings and personal contacts go to make up this often cited exchange of information and experience and help build mutual trust. This is particularly important, since trust is not something you can simply transfer to new partners; it has to be earned. In contrast, the uncontrolled proliferation of such cooperation models jeopardizes their relationships of trust and should therefore be avoided. It is particularly important for all partners to be on an equal footing. The core element, however, is the classic win-win situation. Every partner hopes and expects to find support in their emergency situation and must therefore also be prepared to support the others.

A Worthwhile Investment

Against this backdrop, it becomes clear that the global aspect of information technology also has enormous potential for bilateral and multilateral cooperation. Investing in active cooperation promotes an organization's own long-term effectiveness. We are not alone!



A Career in the Public Sector – The Prospects Are Bright!

For 90% of German workers aged between 25 and 29 who have children, the criterion of family-friendliness is just as important as that of salary when it comes to choosing an employer.[9] Family-friendliness is a high priority at BSI. By offering flexible working hours models and teleworking, we enable our younger employees in particular to create an optimal balance between family and career. Children or career? This is a question you won't hear at the BSI.

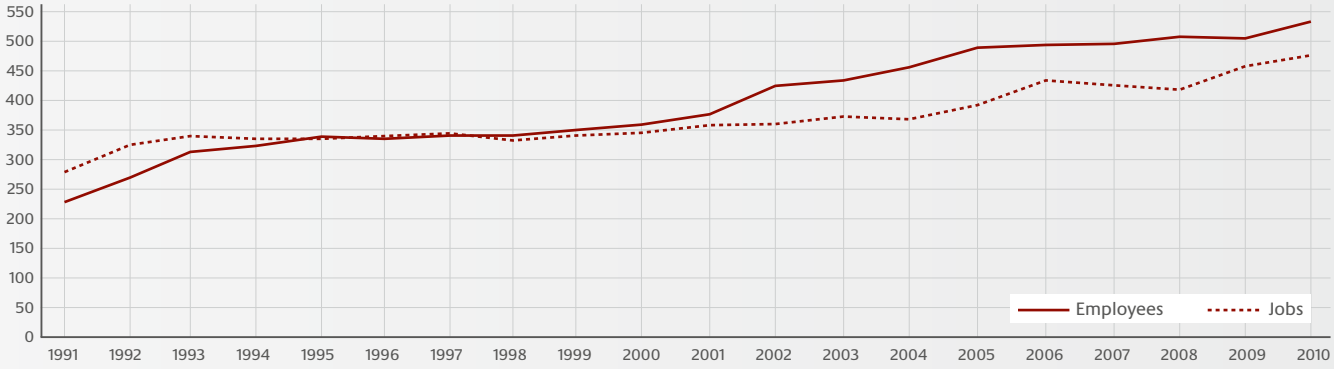
Another trend that is increasingly in evidence at the BSI is that of gaining additional qualifications while working. Many BSI employees are taking on this challenge, and the BSI supports their commitment by, for example, offering flexible working hours to suit their studies.

We also make a point of factoring in the employees' higher qualifications in our strategic human resources planning at an early stage. And this is already paying off: several of our staff who recently completed degrees have competed successfully in job selection processes and have been able to climb up a rung on the career ladder. The BSI is committed to maximizing public-sector career development opportunities for competent, dedicated people.

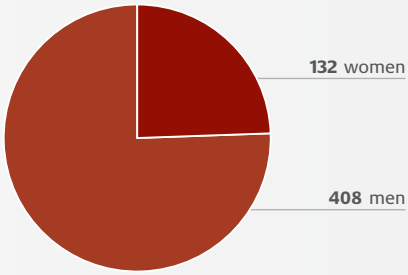
[9] Human Resources Marketing Study 2010 by the Federal Ministry of Family Affairs, Senior Citizens, Women and Youth

Development of Jobs and Workforce at BSI

(Jobs excluding part-time staff, secondees to BSI and trainees)

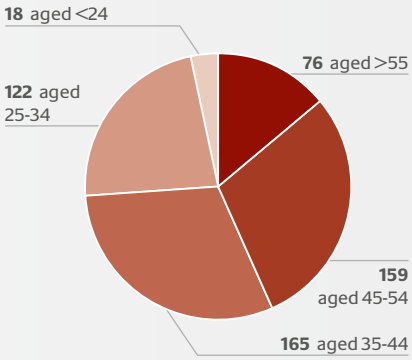


Employees (end of 2010)



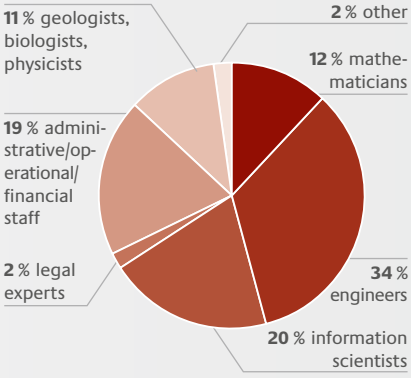
Total: 540 employees

Age Structure

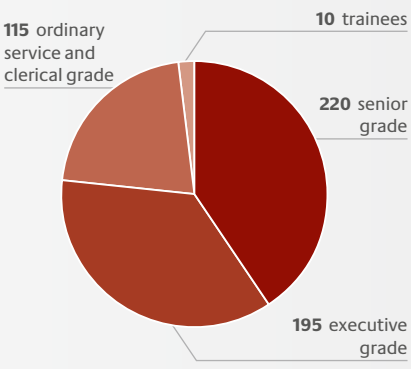


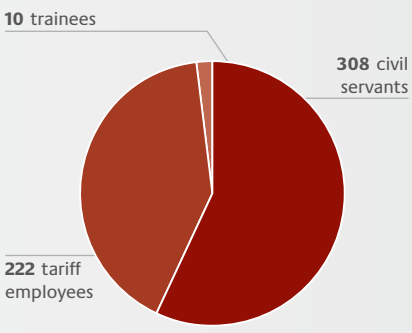
Professional Background

(senior and executive grade only)



Careers





BSI Is Popular Employer with IT Graduates

As in previous years, the BSI was once again one of the most popular employers in the German IT sector in 2010. IT graduates again ranked us in 12th place behind such well-known companies as Google, IBM, SAP and Microsoft.

Stefanie Euler

Section 125, "IT Penetration Center, Defense Against Internet Attacks"

To improve my career prospects and enable me to move up to an executive grade, I decided to follow my training as an IT specialist in system integration with a part-time degree in Business Data Processing at the Cologne and Dortmund Universities of Applied Sciences. As practical experience is very important in IT, the course was perfect for me with its combination of distance and campus learning. I was able to continue working full-time at the CERT-Bund Operations and Analysis Center at the BSI, allowing me to combine the theory with practical experience. The BSI encouraged me all the way and enabled me to organize my working hours and holidays flexibly, which was particularly important for me as my exams loomed.

Just before I graduated, I had a baby. I returned to work after a year's maternity leave, and finished off my degree coursework and bachelor's thesis a little while later. I had already found the subject of my thesis at the BSI Operations Center, so I was able to do some of the practical work during working hours – which made things a lot easier for me.

Because the BSI agreed to let me to go back to my original job at CERT-Bund part-time, it was easy for me to combine career and family. I wanted to be able to put the qualifications I had gained to even better use, so I kept an eye on the executive grade vacancies. A short time later, a suitable vacancy came up in Section 125, IT Penetration Center, Defense Against Internet Attacks. BSI employees who want to change jobs have to go through the same recruitment procedure as everyone else, but naturally it helps to know prospective bosses and colleagues from previous projects. My application was successful and I made a good impression at the job interview, so I was offered a permanent executive grade position immediately after I graduated. To be able to better combine my new job with my young family, the BSI allowed me to increase my part-time hours flexibly to 80%, with a proportion of teleworking. Working from home saves me a great deal of time as I do not have to commute and I can organize my working hours relatively flexibly. And I can spend the time I save with my daughter.

I was initially concerned that as a "part-time mother" I would not be regarded as a fully-fledged member of staff, but fortunately there was no need to worry. Right from the first day I have been working in all kinds of fascinating areas, which motivates me to perform to my best ability. The BSI also encourages part-time staff to undertake continuing professional development, and has given me some exciting opportunities such as taking part in international conferences and trainings. Having had such positive experience at the BSI so far, I am confident that I will be able to continue to work on interesting projects and organize my working hours around my family – which will soon consist of two children.

Pilot Project: Academic Support

There is a shortage of IT specialists at executive grade level. Together with four other authorities in the Federal Ministry of the Interior's area of operations, the BSI has launched a pilot project to nurture young IT specialists at executive grade level. Since 2008 the BSI has sponsored Bachelor's degree students with grants, and guarantees them a permanent job when they graduate. The first student to receive this support, Sebastian Cielewicz, is a former BSI trainee. He will graduate in Computer Science at the Bonn-Rhine-Sieg University of Applied Sciences next year, and will then work for the BSI at executive grade level.

Sebastian Cielewicz

What gave you the idea to apply for the BSI academic support program?

Cielewicz: Before the application processes for the academic support program started, I had a temporary job at the BSI, having trained as an IT system engineer. My training manager at the time told me about this program. I immediately thought it was a great idea and applied straight away. I particularly liked the prospect of a permanent job at the BSI after I graduated, as I very much enjoyed working there. The working atmosphere is great, and everyone is really nice and helpful. There are lots of interesting and challenging tasks.

How does the Academic Support Program work?

Cielewicz: Once the application process has closed and an applicant has been chosen, the applicant has to apply for a place on a course and enroll at Bonn-Rhine-Sieg University themselves. You get your tuition fees refunded when you submit the receipts. You also have to provide proof that you have obtained the exam credits every semester. While you are studying, you get a monthly grant from the BSI that is the equivalent of the maximum government allowance. Once you get to the point where you have to choose your specialism later on in the course, it is a good idea to discuss your choice with the student support manager. This gives both sides an opportunity to look at where you could potentially work in the BSI once you graduate. The BSI not only offers you the internship you need to do as part of the course but also a position that will be useful for your bachelor's thesis.

How do you rate the program so far?

Cielewicz: I rate it very positively so far. On the content side it gives me enough freedom to choose the subjects I want to focus on on the course. You don't get pushed in a particular direction; you can choose the area you are most interested in. Personally I have never regretted joining the program. The advantages are obvious: it's a great combination of theory and practice. With my training and my job I already have quite a lot of background knowledge that helps me on the course. And vice versa: I can put the things I am learning on the course to practical use in my internship at the BSI and gain more practical experience. And the BSI also benefits: interns can apply all the latest findings and developments they learn about on the course in their work, and new people can be recruited at an early stage. Of course, a very big advantage for me is the security of knowing that when I graduate, I am guaranteed a permanent and interesting job at the BSI that matches my qualifications.

How do your fellow students react when they hear that you get a student grant and have secure job prospects?

Cielewicz: The ones who know about it think it's great – in fact they are a bit envious! These days it's quite something to have a secure job prospect. And my colleagues at the BSI whom I've told about it also think it's a good thing.

BSI – 20 Years

“20 Years of the BSI – Recognition and Thumbs Up“

Peter Hohl, journalist and founder of SecuMedia Verlags-GmbH

On December 17, 1990, the day on which the BSI Act was announced in the Bundesanzeiger[10], I was sitting at my PC writing a report about the Federal Office, which was to start operating under its new name on January 1, 1991. The word “internet” came up in my report. When I ran a spell check, my word processor thought it was a spelling mistake and suggested replacing it with *“internat”*[11]. Which just goes to show that state affairs can sometimes be one step ahead of the world of computers and programs.

And so the BSI was born, and started operating as an independent higher federal authority with the same staff as in its predecessor department. I have been lucky enough to work with the BSI throughout the whole of its history. As I browsed through the annual volumes of <kes>[12] for material for this article, a couple of aspects of the anniversary got me thinking. Above all, I asked myself the following:

What are the main differences today compared with the early days, and could we perhaps use them as pointers? Three things struck me in particular:

1. Obviously, the omnipresence of IT and the internet, or Pervasive Computing as one of the BSI studies is called. A government without a massively strong skill base in this crucial area would be inconceivable in a civilized country.
2. Twenty years ago, security was primarily a response to concrete threats. First there were viruses, then there were antivirus programs; first there were hacker attacks, then there were firewalls. “Security” was first and foremost a noun describing something concrete. And it still is today. But there is something else as well now. “Secure” as an adjective – describing a necessary feature of a completely different product or process. It was not the design of the new ID card that discussions revolved around, but its security. Concerns surrounding social networks are not about philosophical or social issues but about data security. No one doubts that web applications or cloud computing work. But how secure are they?
3. The intensity with which security is questioned and discussed nowadays. Think about online banking, the process of obtaining your own credit rating, or electronic mail. All have highly complex and complicated security procedures. I have tried them myself. And people clearly no longer view these procedures as an imposition but as a positive criterion in their decision to use the products or services.

Looking back, we can trace a path of tumultuous development that started even before the BSI was established. I went to the Hannover Fair for the first time in 1978. I was only interested in one hall, which was called the Center for Office and Information Technology – abbreviated to CeBIT. I was looking for a word-processing system for the publishing house I was in the process of setting up. And what did I find? A system that had something that previous systems did not have: a screen. Hence its German name, BITSY, which stands for BIldschirm-TextSYstem, or screen-based text system. It had no hard drive – those were very much the preserve of mainframe computers at the time – but instead of the music cassettes that most systems had, it had two drives for Minifloppies. Later these would be known as 5¼” diskettes. Storage capacity: 80 kilobytes. The operating system was on one, and the data were on the other. RAM: 19 kilobytes. Cash price: DM 32,000.

[10] Official Gazette of the Federal Republic of Germany
[11] Boarding school
[12] SecuMedia Verlags-GmbH Information Security Journal

Peter Hohl with his BITSY some 30 years ago

Another thing that made an impression on me before the BSI was set up was a story kicked off by a certain American called Fred Cohen – almost at the same time as a German, as it later turned out. In November 1984, *Der Spiegel* ran a 10-line report: Fred Cohen had written a program at the University of Southern California that could conceal itself in other programs and cause the infected computer to spread copies of itself. Because it behaved very similarly to a virus, that was the name he coined for it.

I found that quite worrying, and not being part of the tabloid family, we feel a sense of responsibility for what we do. In other words, we thought long and hard about whether we should put the information in the public domain. But shortly afterwards an underground paper called the Bayerische Hackerpost wrote about this new form of attack, so we knew it was time to let EDP security managers know what was going on.

So we published articles on the new happenings in the next two issues of <kes>. The report was illustrated with a caricature that predicted a return to the Stone Age. That we didn't return to the Stone Age – and that is my firm conviction – is largely thanks to the BSI, who faced up to the challenge and for many years was the pivotal source of information for virus issues before an effective and reliable antivirus industry got off the ground. But now let's jump to 1991. The BSI was up and running. My first visit to the new authority took place at a quite well protected property in Mehlem. What we wanted to know was how open the agency would be towards the public in the future. The answer was: very open, as far as most of its tasks were concerned. Even then it was being considered whether the BSI should have its own organ.

Does anyone remember August 20? That was the day of the Soviet coup d'état attempt in Moscow. Soviet President Michail Gorbachev was being held at his dacha in Ukraine. Boris Yeltsin climbed onto a tank outside the White House in the Soviet capital and mobilized the people and the military against the rebels. That day, on which the world seemed to wobble, members of the German government were in a state of high alert and did not budge from their command centers. But for one minister, another event was so important that he didn't cancel his appointment: Wolfgang Schäuble presented the president of the BSI with a brand new building on August 20. A building with a glass facade – symbolizing the openness of its future work. Sometimes you can illustrate a point nicely by asking: What would the world look like without it? Without the BSI, there would be no Grundschutz, no certification, no BSI-für-Bürger website; many books, many studies, and many CDs would never have been produced. And there would very likely be no European counterparts.

All in all, the BSI has achieved an enormous amount in all areas and at all levels over the past 20 years. And from my own perspective, I would like to add this: the three letters "BSI" after a name are a very special reason to be proud. The reputation and respect the BSI staff have earned – again, at all levels, and not just through their personal competence but also through their authority's reputation for technical expertise and integrity – is quite remarkable.

Their biggest achievement, which will not appear in any statistics, is worthy of particular mention here: During these past 20 years, the BSI has won the trust of the public. And these days that is a treasure of inestimable value. And so I firmly believe that the achievements of the BSI and its team over the past 20 years deserve great recognition – and a big thumbs up for the future!

Peter Hohl is a journalist, founder of SecuMedia Verlags-GmbH and publisher of <kes>. He organizes the it-sa IT security trade fair in Nuremberg and has been closely associated with the BSI since its foundation.

"Outstanding technical expertise and a highly motivated team"

Interview with former BSI presidents Dr. Otto Leiberich, Dr. Dirk Henze and Professor Udo Helmbrecht

What were the historical and personal highlights of your time at the BSI?

Dr. Otto Leiberich: It was the time when the BSI was being set up. It was established on January 1, 1991, and I was appointed as president. The BSI's predecessor authority worked exclusively on state security. But with the BSI Act came responsibility for IT security in the commercial and private user spheres as well. Taking on this task was a major challenge.

Dr. Dirk Henze: I can only really answer this question by saying that I am delighted that during my time in office the BSI underwent a continual process of expansion from its traditional tasks to becoming a central IT security service provider for the federal government, and that we helped anchor IT security firmly in our national security culture.

Prof. Udo Helmbrecht: I remember the May 2004 spam attack that paralyzed our government network. It took days to get IT operations back up and running normally again. That was also the beginning of the long-term development and expansion of CERT-Bund. Another exciting aspect was the introduction of the electronic passport and the discussion around the security of the RFID chip and data protection that came with it. It was also interesting to experience a change of government in 2005 from the inside out, so to speak. And the 2009 amendment of the BSI Act was an important milestone for the future development of the BSI.

What memories do you have of your first 100 days?

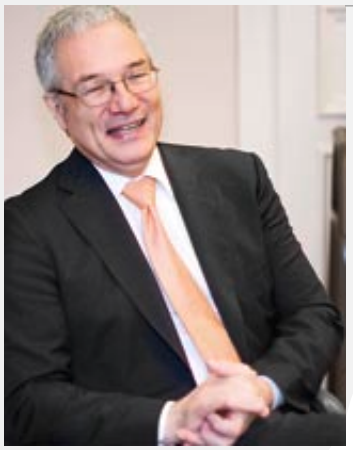
Leiberich: The years before the BSI was established were difficult ones. "Project BSI" had many opponents and often teetered on the brink. Returning to the old situation would have had severe personal consequences for my closest allies and myself. But we achieved our goal, and the BSI came into being. So I look back on my first 100 days as a time of liberation from very intense pressure. There was a feeling of optimism in the air. We went about our work with enthusiasm and commitment. We were united by the feeling: "We'll do it!"

"I think the establishment of the BSI was ahead of its time."

Dr. Dirk Henze, BSI President from 1993 to 2002

Henze: I found a well-oiled and efficient administration when I joined. After 23 years in the Federal Ministry of the Interior, heading up the BSI's specialized departments was something of a culture shock for me to begin with: the staff were highly competent and dedicated, but I found a rudimentary vertical and horizontal flow of information, and people would put forward very individual ideas that had not always been agreed with superiors.

Helmbrecht: I got a lot of support, which made it much easier for me to find my feet. I was particularly impressed by the commitment of the BSI staff and the way they identified with the organization. The *"Erlass"* (implementing directive) and the processes associated with it were something completely new for me. For someone who grew up in industry, that takes some getting used to.



"I was particularly impressed by the commitment of the BSI staff and the way they identify with the organization."

Professor Udo Helmbrecht, BSI President from 2003 to 2009

Where do you think the BSI will be in another 20 years?

Leiberich: I don't like forecasts, as they usually turn out to be wrong. But in this case I'm sure: the future of IT will depend on whether we are able to keep cyber crime in check. And the BSI will be fighting on the front line. So it will grow in importance. What's more, the BSI has built up outstanding subject expertise over the years. This is something I have found out from technical discussions with young colleagues, so I have no worries about its future.

Henze: Both Winston Churchill and Niels Bohr are said to have said that "Predictions are difficult, especially about the future". They are an excellent arena for charlatans, because their claims are usually impossible to prove or refute. I suspect that preventive and operational tasks to fight IT crime will ultimately move closer towards each other from an organizational point of view. I also believe that as a result of new findings, consolidation and cost pressures, the BSI will have to adjust to a discussion of genuine state tasks in the area of IT security.

How did the relevance of IT security in society change during your time at the BSI?

Leiberich: The prevailing opinion of many business people was, and, sadly, still is: "As long as an IT security system costs more to run than the annual cost of the damage, I won't be investing in one." They shut their eyes to the risk of serious damage. Shades of Stuxnet. But something that is causing me even more concern is the Wikileaks phenomenon. If everyone who bears a grudge against their employer can simply take information and share it without running the risk of being caught, our efforts are wasted. The most secure encryption in the world is useless if the original text is revealed.

Henze: My time at the BSI – almost 10 years – was characterized by the increasing complexity of the worldwide network of IT systems. When the internet started to be used free of charge on a large scale in 1993, a whole range of new threats came into being that affected the state, society, businesses and private individuals. The almost daily press releases about IT glitches and criminal abuses, particularly in relation to online banking, really brought the subject of IT security home to a wide public. In addition, the growth in staffing levels and financial resources at the BSI during this time proves that the subject had even reached Parliament.

Helmbrecht: The BSI has always been highly respected in the IT sector. In the BSI-für-Bürger website and Bürger-CERT we created services that bring IT security home to the private user. IT-Grundschutz, Common Criteria Certification and our Technical Guidelines have increased the level of IT security in the private sector as well. Protecting against IT threats is a top priority today.

What role did the international dialog play in your time?

Leiberich: In my time at the BSI, none. I can't remember any other European countries having equivalent authorities. They were still lagging behind us at the beginning of the 1990s.

Henze: International cooperation was largely restricted to the exchange of information with state agencies operating in a different field than the BSI. I think the establishment of the BSI was ahead of its time. The advantage was that it could play a pioneering role on the international stage.

Helmbrecht: IT threats are global. Cooperation with the security authorities in our partner countries is eminently important. Mutual trust plays a major role in this context. A partnership has developed between the CERTs, enabling information on IT attacks to be exchanged early on and allowing the state to take prompt action.

How important was it to communicate with private users in your time? How do you think this has changed?

Henze: Information technology only really reached the private user with the advent of the internet. This is an area where help is really needed, and the BSI now does a lot to deliver that help.

Helmbrecht: It was always important to me to communicate with all stakeholders in society right from the start. These days computer technology is used in all spheres of life. Administration processes are being modernized – an example of this is the electronic tax return. The new ID card with the RFID chip is being used in private and public sector processes. But as a result, the state also takes on responsibility for IT security. Communication means transparency and engenders trust in the use of the new technologies.

What do you miss about your time at the BSI? What fond memories do you have?

Leiberich: The technical side of the work and working with a competent and highly motivated team.

Henze: I have always liked dealing with people from so many different spheres and with so many different mentalities. I have fond memories of that.

"The years before the BSI was established were difficult ones. 'Project BSI' had many opponents and often teetered on the brink."

Dr. Otto Leiberich, BSI President from 1991 to 1992

Helmbrecht: I miss the many personal conversations, getting together after events, the trade fairs that gave me an opportunity to exchange ideas with colleagues. I have fond memories of always being able to rely on the executives and staff at the BSI.

Do you have any not-so-fond memories?

Leiberich: I have always regarded myself more as a practitioner than an administrator. My aim was to know exactly what was going on in all specialist areas so that I could help make the appropriate decisions to steer our course. What I was less keen on was appearing in public, such as before Bundestag committees, the Court of Auditors, the Finance Ministry or the press. These appearances may have earned me recognition, but they caused me sleepless nights.

Helmbrecht: Nothing really springs to mind!

How did your role as president of the BSI affect the way you used information technology in your private life?

Leiberich: I owe information technology a great deal. After I left office, I spent a while working as a consultant to new IT companies and in research. That would have been impossible without a computer and the appropriate software. But I admit that I may have taken the odd liberty with security myself. After a short time I threw all the precautionary measures I so often used to preach to the wind. And I paid a tough price: one day a virus knocked out my computer. There was nothing I could do to get it up and running again. I didn't want to ask my former colleagues for help as I couldn't face the jibes! And to make matters worse I was lazy about backing up my data, so I lost some valuable files.

Henze: As a student trainee back in 1959 I learned the programming language for the Zuse Z22. Later on I spent decades working on promoting innovative IT applications, in which IT security featured much less prominently, as it was in those days. Today the way I use IT in my private life is shaped very much by these experiences and by my awareness of IT security issues.

Helmbrecht: I am much more aware of how I use my computer, and I talk to my family and friends about IT security whenever it's appropriate.

A Look Back Over the Other Events of 2010

A Review of 2010

January

January 19-21

Omnicard 2010

As part of the federal government's eCard strategy, which includes the electronic passport, ID card and health card, the BSI is the point of contact at Omnicard in Berlin for all questions relating to IT security.

January 27-28

LÜKEX 2010

The BSI takes part in LÜKEX, the National Crisis Management Exercise.

February

February 4-5

COSADE 2010

The First International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE 2010) in Darmstadt is organized by CASED and the BSI.

February 9

Safer Internet Day

To mark the EU's Safer Internet Day, the BSI answers questions about internet security on a toll-free telephone hotline.

March

March 4-9

RSA Conference in San Francisco

The BSI presents its services and projects on a joint German stand organized by TeleTrusT on behalf of the Federal Ministry of Economics at the RSA Conference in San Francisco.

March 2-6

CeBIT 2010

The BSI has a stand at CeBIT 2010 and runs a series of workshops at the Convention Center. Among the subjects presented are Security on the Internet, IT Grundschutz , Secure Mobile Solutions, IT Security Certification and Security of Government Documents. (photo)

March 16

1st IT Grundschutz Day

The first IT Grundschutz Day 2010 in Bonn focuses on the subject of "Virtualization of IT Systems – Risks and Dependencies"

April

April 22
Annual Meeting on Security of Classified Information

At the invitation of the BSI, the Federal Academy of Public Administration (BAköV) in Brühl near Cologne organizes the first annual meeting on Physical and IT Security for Classified Information. This meeting is aimed at employees of federal and Länder authorities responsible for the physical and IT security of classified information.

April 22
Girls' Day

The BSI takes part in the 10th nationwide action day for girls with talks and presentations on the subject of "Bits and Bytes for Girls".

April 27-28
Efficient State

The BSI exhibits at the 13th German Administration Conference, "Efficient State", providing information on the STORK project (Secure idenTity acrOss boRders linKed). The BSI represents the Federal Republic of Germany in this EU-funded large-scale pilot project.

April 27-28
Interdisciplinary Symposium

The Working Party on Identity Protection on the Internet (a-i3) and the BSI organize a symposium on "Secure Identities, Data and Services: eCards – De-Mail – Cloud Computing – Patient Data" in Bochum.

May

May 5
SOA Workshop

The BSI's first workshop on the subject of "Security in Service-Oriented Architectures (SOA)" takes place in Bonn.

May 12
BKA/BSI Business Conference

The business conference organized by the Bundeskriminalamt and the BSI on the subject of "Cyber Crime – A Global Danger?", is attended by representatives of the federal and Länder security authorities and businesses.

May 19
RFID Workshop

The BSI runs a public workshop on the subject of "Technical Guidelines for Secure Use of RFID". (photo)

June

June 9-12
LinuxTag 2010

At LinuxTag in Berlin the BSI presents its latest IT security solutions based on Free/Libre and Open Source Software (FLOSS).

July

July 1

Call for Papers

Call for Papers opens: the subject of the 12th German IT security conference to be held in Bonn in May 2011 is "Securely into the Digital World of Tomorrow".

August

August 21-22

Invitation to visit the government in Berlin

The Federal Government's 12th Open Day takes place in Berlin under the motto "Invitation to Visit the State". The BSI presents its IT security information services for the public.

September

September 15

Anti-Botnet Advisory Center Opens

The Anti-Botnet Advisory Center is open for business. Operated under the auspices of the eco-Association of the German Internet Industry, the Anti-Botnet Advisory Center is a point of contact for internet users whose computers are infected with a botnet.

September 21-23

11th ICCC

The BSI takes part in the 11th International Common Criteria Conference in Antalya, Turkey, with certification awards and papers.

September 24

2nd IT Grundschutz Day

The BSI's second IT Grundschutz Day, run in cooperation with HiSolutions AG, takes place in Berlin with the theme "Certification from Various Perspectives". (photo)

September 27-28

Annual Meeting for IT Security Officers

BSI and the Federal Academy of Public Administration (BAKöV) hold their joint annual conference for IT security officers of federal authorities.

October

October 5-7
ISSE 2010

At the Information Security Solutions Europe (ISSE) in Berlin, the theme of the BSI's stand and workshop is the new German ID card.

October 5-8
Security Fair in Essen

At Security 2010 in Essen the BSI presents its consulting and general services around IT security and offers advice on subjects including physical IT security and IT Grundschutz for SMEs.

October 6-7
PITS 2010

Under the motto "Security in Virtualized Environments", the Public IT Security (PITS) conference and trade fair for the public sector takes place in Berlin. BSI experts take part in various forums.

October 19-21
it-sa

The BSI takes part in the leading IT security trade fair it-sa in Nuremberg, with a stand, various papers and a BSI IT Grundschutz Day.

October 20
3rd IT Grundschutz Day

Under the motto "Efficiency and International Orientation in IT Grundschutz", the third IT Grundschutz takes place at it-sa in Nuremberg in collaboration with TÜV Informationstechnik GmbH.

October 27-28
Modern State 2010

Subjects of BSI presentations at the Moderner Staat trade fair in Berlin are IT Security Consulting, IT Grundschutz and IT Audits. The BSI also runs a series of workshops.

November

November 1
Launch of nPA

The new ID card (nPA) is launched across Germany.

November 16
EICAR Conference

The BSI hosts the conference of the EICAR (European Institute of Computer Antivirus Research) Working Group WG2, focusing on information exchange on malware and antivirus programs between administrators, IT security managers and manufacturers.

November 25
German IT Security Prize

Award ceremony for the Third German IT Security Prize under the patronage of BSI President Michael Hange.

November 25
4th IT Grundschutz Day

The 4th IT Grundschutz Day 2010, on the subject of "Security Aspects of Cloud Computing", takes place in Darmstadt together with the BSI's cooperation partner Fraunhofer SIT.

December

December 6-7
ZertiFA 2010

The BSI runs workshops at ZertiFA 2010 in Berlin.

December 7
5th National IT Summit

The BSI takes part in the 5th National IT Summit in Dresden.

Picture credits
BMI, BMWI, BSI, BSI employees, Deutsche Messe Hannover, eco, Eric Lichtenscheidt, European Commission, LinuxTag/Messe Berlin, Shutterstock, Susanne Stark, T-Systems/HTC, SecuMedia/Peter Hohl, secunet/Lenovo, STORK

Publisher
Federal Office for Information Security BSI
53175 Bonn, GERMANY

Project Manager
Anke Gaul

Text and Editorial Staff
Federal Office for Information Security BSI
DauthKaun Werbeagentur

Layout and Design
DauthKaun Werbeagentur

Printed by
Druckpartner Moser, Rheinbach

Date
July 2011

Article Number
BSI-JB11602e

Distribution Office
Federal Office for Information Security BSI
Section 321, Information and Communication, Public Relations
Godesberger Allee 185-189
53175 Bonn, GERMANY
Phone: +49 228 99 9582-0
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de