Federal Office
for Information Security

Security in focus

BSI Magazine 2015

HELPING PEOPLE TO HELP THEMSELVES

Modernising the IT-Grundschutz

A SAFER INFORMATION SOCIETY

The IT Security Act comes into force

Contents

Cyber Security

A Safer Information Society

IT Security In The Field

The Federal Office For Information Security And Its Tasks

Editorial

Dear Readers,
The IT Security Act has been passed by the German parliament, the Bundestag. It now needs to become established in companies and also in society. The new legislation grants additional rights and obligations to the Federal Office for Information Security. We will actively use these to support the establishment process and improve the robustness of our critical IT infrastructures.

These infrastructures are more vulnerable to attack than ever before. More and more devices and machines are now connected to the Internet, along with more and more areas of our lives and productive activities. Extensive risk analyses are required in order to properly assess the dangers and minimise the probability of their occurrence. Clear guidelines in the field of IT security, as defined in the new legislation, help companies to establish a solid foundation on which to build.

In recent years, we have witnessed a rapid increase in attacks, which are becoming increasingly sophisticated. The hacking of the German parliament's IT systems and the DDoS attacks on the German Federal Chancellor's websites are just two such examples. Both the quantity and the quality of cyber attacks are constantly changing and adapting to the current realities of cyberspace. But it still holds true that solid basic protection prevents the most common attacks and forces attackers to use newer methods which cost more and make their efforts economically pointless.
IT security and cyber security are becoming increasingly important issues in our everyday lives. Whereas up to now the focus has been on user-friendliness and intuitive operation, an awareness of security is now notice-ably on the rise. It is time for this subject to become more firmly established in the public consciousness. This magazine offers an insight into selected projects that aim to ensure precisely that. I hope you find the read interesting with plenty of food for thought.
Bonn, September 2015

Michael Hange

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

Every piece of the mosaic

Keeping a constant eye on the current threat situation

The Federal Office for Information Security publishes a report every year entitled “The State of IT Security in Germany” which provides information on the current IT security situation in Germany. The report seeks to deliver robust answers that go beyond speculation and hysteria – a challenging task that involves many experts from the Federal Office for Information Security spending months putting together countless pieces of a mosaic, analysing them and then evaluating them in order to deliver an up-to-date and well-reasoned response to the question: “what is the current cyber security situation?”.

On 17 December 2014, Dr Thomas de Maizière, Federal Minister of the Interior, and Michael Hange, president of the Federal Office for Information Security, presented the report “The State of IT Security in Germany 2014”. The aim of the report was to provide insights into the IT security situation in Germany and to make the Federal Office for Information Security’s evaluation of these insights accessible to the wider public. This was not just about informing readers and raising their awareness – it was also primarily about demonstrating that each and every user has individual responsibility for IT security. A large project team worked with many experts from the Federal Office for Information Security to produce the 40-page report.

02
01
03
05
04

→ Assessing the situation and collecting information

Nowadays, not a day goes by without media reports on cyber attacks, new technological weaknesses, disruptions of IT processes and data leaks. Every message, every report and every statistic is a piece in the mosaic which needs continuous reassembling to gain a picture of the situation.

Evaluating information sources

Primary sources are represented by the knowledge gained by the Federal Office for Information Security Situation Centre, the Computer Emergency Response Team (CERT), the federal administration and the Cyber Response Centre, and also information from day-to-day operations in the specialist departments. In addition, there is the Federal Office for Information Security’s own sensor data which is generated, for example, from the protection of government networks. Information obtained from third parties is also of considerable importance, along with the evaluation of a variety of public information sources which are used by experts at the Federal Office for Information Security, especially for situation monitoring.

Technical parameters and organisational frameworks

The status report published by the Federal Office for Information Security does not only give a view of the technical parameters. Constantly evolving framework conditions also have a significant impact on the situation, e.g. how information technology is currently being used in business or private contexts. Then there are the causes behind the current risk situation that are more organisational than technical in nature. Following publication of the report in December 2014, there was a widening of the debate around IT security, particularly in the political arena, to include aspects such as “digital carelessness”. This expression describes the everyday conflicting relationship between the responsibility and carelessness shown by users when handling information technology.

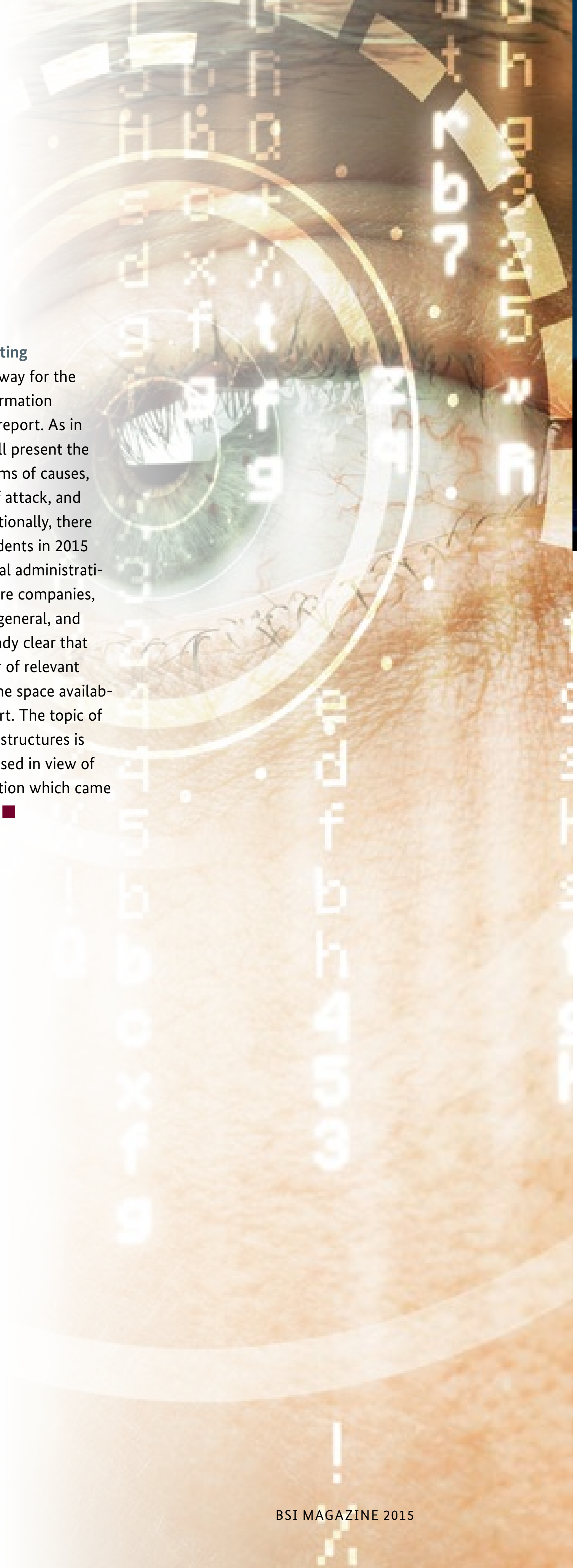
Thus, the continuous analysis of technical parameters, an understanding of organisational influences, and consideration of current framework conditions are the basis for a well-substantiated annual report on the IT security situation in Germany.

Expert analysis

In addition to the gathering of information, expert knowledge is also required, particularly at the evaluation stage. Only an expert who has devoted a great deal of time and effort to a subject can separate new information from that which is already familiar, or sort facts from speculation. An expert is able to properly classify the dependability of an information source and by doing so come to a reliable assessment of the situation.

Cyber Security Situation Overview – basis for the status report

The basis for the Federal Office for Information Security’s status report in its current format is provided by the Cyber Security Situation Overview published by the Analysis and Trends Section of the Cyber Security Department. This evaluation document has been produced regularly since spring 2014 and has examined nine different topics to date. It serves as the internal basis for the status report. The goal is to further improve the evaluation of the situation. To this end, analysis processes have been better formalised, more sources have undergone continuous monitoring rather than on an ad-hoc basis, and a situation report on key topics has been created that is always up to date. As well as being used internally, the information from the Cyber Security Situation Overview will also appear in the member area of the Alliance for Cyber Security website for participants in the initiative.



→ **The status of IT security in Germany in 2015**

The Federal Office for Information Security's 2015 status report will be published in autumn 2015 and will provide an updated answer to the question: "what is the current cyber security situation?".
It is then up to readers to actively take individual responsibility and translate the report's findings into practical action to improve IT security. An understanding of the current situation is essential to be able to respond to it appropriately.

Daniel Mühlenberg, specialist advisor in the Analysis and Trends section

Non-stop status reporting

Work is already under way for the Federal Office for Information Security's 2015 status report. As in the previous year, it will present the current situation in terms of causes, means and methods of attack, and types of attacker. Additionally, there are the reports on incidents in 2015 that affected the federal administration, critical infrastructure companies, the business sector in general, and private users. It is already clear that once again the number of relevant incidents will exceed the space available for them in the report. The topic of protecting critical infrastructures is also likely to be addressed in view of new IT security legislation which came into force in July 2015. ■

One per cent insecurity is too much.

Penetration testing and internal audit

By Sebastian Schreiber, managing director of SySS GmbH

The inspection of IT, and IT security in particular, still plays a less significant role in internal auditing, but is steadily becoming more important – and for good reason. Companies have long implemented a variety of measures to safeguard IT security ranging from various certifications in accordance with ISO and the Federal Office for Information Security through to audits of all kinds. Reports of IT security incidents in organisations, companies and public authorities continue to make the headlines with recent prominent examples being the hacking of Japanese company Sony in December 2014 and of the German Bundestag in June 2015.

These IT security incidents explicitly demonstrate that even the IT systems of international high-tech companies and senior government institutions are not adequately protected.
Widely used IT quality assurance measures – including code reviews, the Security Development Lifecycle or IT-Grundschutz and ISO certification – may be sufficient to secure 99 per cent of these systems. But the crucial point is, however, that the resulting one per cent vulnerability that remains is a target for digital attacks. A single gap, however small, is enough to render an otherwise well secured IT infrastructure open to attack in its entirety.

Qualified computer scientist Sebastian Schreiber, born in 1972, studied information technology, physics, maths and business studies at the University of Tübingen. He worked at Hewlett-Packard from 1996 to 1998. Schreiber founded SySS GmbH in Tübingen while still studying for his degree. Since 2000, he has regularly appeared at trade fairs and conferences in Germany and abroad as a live hacker. He is a popular IT security expert in the print media, in broadcasting and on Germany's Jauch television talk show. He is a long-standing member of the Baden-Württemberg Association for Security in Business and also a member of the advisory board of the journal Datenschutz und Datensicherheit (Data Privacy and Data Security).

SySS GmbH is inextricably linked with penetration testing. It was first carried out here in 1998. The company now employs over 70 people and is the market and technology leader in this field within Germany and Europe. In addition to security testing, the company's portfolio also includes digital forensics, IT security training and live hacking.

A penetration test simulates hacker attacks. In a test, the tester takes on the role of an attacker in order to detect security flaws.

Penetration tests are a quick, cost-effective and straightforward way to uncover current security flaws and find workable solutions.

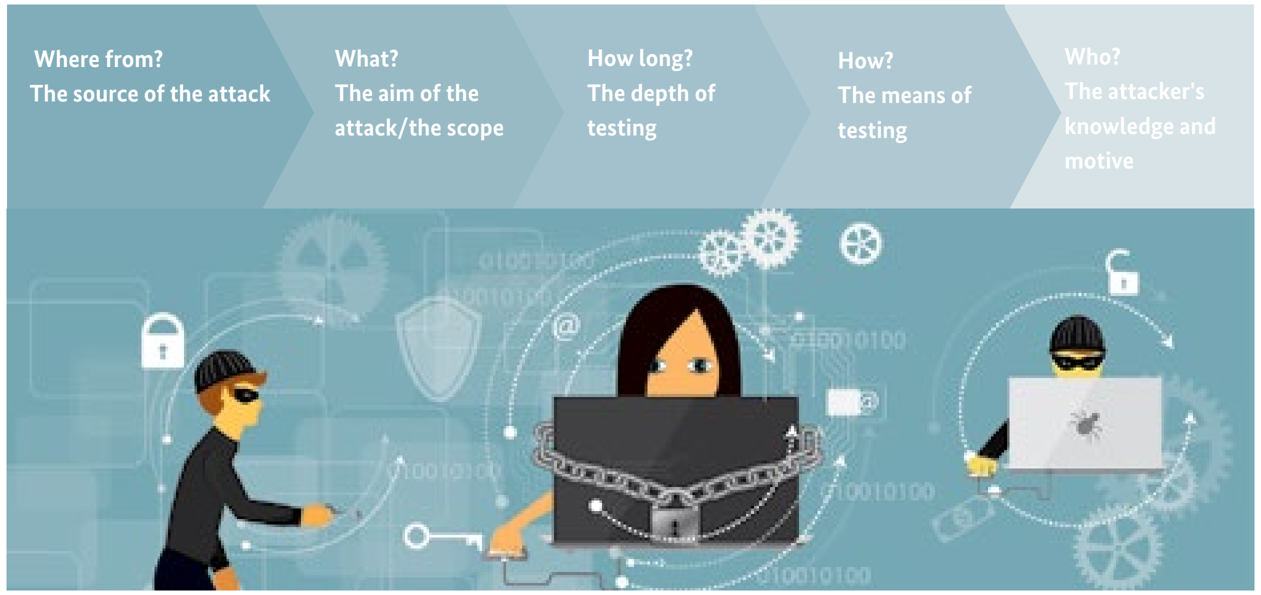
→ Regular simulations of hacker attacks

Real-life attackers' knowledge is based on experience which they are able to use to seek out and exploit this one per cent insecurity. It is precisely at this point – or preferably before it – that penetration testers get involved. To put it simply, a penetration test simulates a hacker attack. By adopting the perspective of attackers who could potentially try to attack a company, the tester is able to detect security flaws before they are exploited in an attack. However, it is important to note that new security flaws appear in software products every day, thus opening up potential new gateways for hackers. Therefore, penetration testing should be firmly integrated into the auditors' inspection schedule and carried out frequently at regular intervals. This ensures that the many different hacker attacks – which the company concerned knows nothing about – are no longer discovered purely by accident. Instead, weaknesses are identified and dealt with in a targeted manner before a system becomes infected by, for example, a Trojan which could remain undetected for years.

A single penetration test examines one or more attack scenarios, which must be clarified in detail before the test begins. The auditor/client defines the following specific requirements for each scenario in relation to the individual company:

- Where from? The source of the attack
- What? The aim of the attack/the scope
- How long? The depth of testing
- How? The means of testing
- Who? The attacker's knowledge and motive

To carry out penetration testing effectively, testers need to keep their specialist knowledge constantly up to date. It is therefore not advisable for these examinations to be carried out solely by the company's own IT department. In-house IT departments usually cover a very wide range of tasks with no specific focus on IT security, and therefore risk becoming blind to the company's weaknesses in the long term. Incorporating an unbiased view from an external penetration tester into regular audit inspections thus helps to expose blind spots and close security gaps before an incident occurs.



An appealing inspection concept

For internal audit departments, penetration tests have other practical advantages in addition to their demonstrably positive impact on IT security: they are quick and cost-effective to carry out and do not entail a large amount of effort for the auditor. Upon publication of the test report, another benefit becomes apparent: the findings of a penetration test are usually impressively clear. The weaknesses identified and their implications leave little room for interpretation and are generally easy to understand, even for people who are not computer specialists. For example, when a penetration tester proves that it is possible to read all the supplier data from a database in just a few hours, nobody can objectively argue against it. Thus it becomes clearly evident at this point that a gap in the company's IT security exists and that immediate corrective action is necessary.
A penetration test is also constructive for the audit department. At the end of every test is a final report which not only documents all the security flaws detected, but also contains concrete suggestions for remedying them. The auditor is then able to present the company IT department with a specification sheet and also conduct a follow-up test with relatively little effort to establish whether the aforementioned security flaws have been successfully eliminated.

At least for the time being, the auditor will then be able to sleep soundly again. It is always important to remember that one of the key differences between the penetration test and other test procedures is that the systems do not receive a "secure IT" seal of approval with a defined validity period. In fact, it is not inconceivable that within just a few days following a successfully completed penetration test, new security gaps will be found somewhere within the world of the Internet to make even recently secured systems again vulnerable. That is precisely why it is so important to systematically integrate penetration testing into planned inspections on a regular basis according to the complexity of a company's IT environment and how vulnerable it is deemed to be. The creative powers of penetration testers means they are able to put themselves in the position of hackers with malicious intentions and think outside the box, thereby detecting weaknesses that other inspection methods might not pick up.

Companies that scrutinise their IT security measures systematically in this way on a repeated basis minimise the risk of becoming a target for hacker attacks. ■

Literature recommendation of the author

Aleksandra Sowa, Peter Duscha, Sebastian Schreiber: IT inspection, IT auditing and IT compliance. The theory and practice of IT testing (Springer Vieweg 2015) This reference book focuses on new instruments and methods used in the work of innovative IT auditors. Taking a modern, risk-oriented audit approach as its starting point, the book deals with a broad range of hot topics including data protection, cyber security, penetration testing and investigations. A useful guide for practitioners involved in planning and carrying out inspections.

National Cyber Response Centre

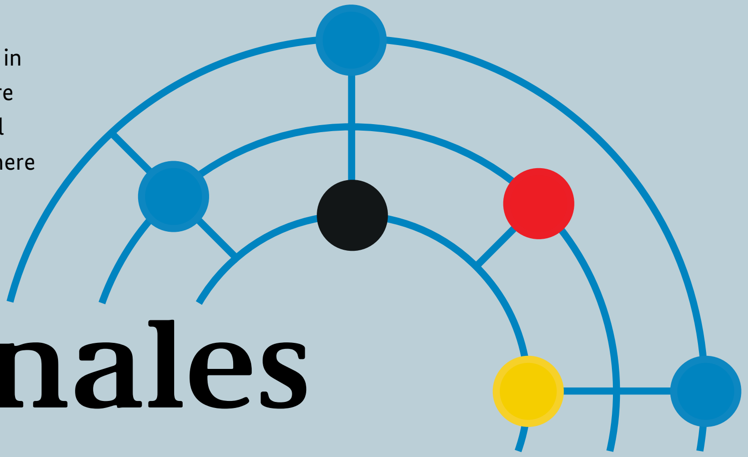
Jointly shaping IT security

The complex threats to IT security in the Federal Republic of Germany extend beyond the German security authorities' firmly established boundaries of responsibility. As a result, neither the Federal Office for Information Security nor any other organisation is able to provide on its own an optimum response to the dynamic threat situation. It is therefore all the more important to maintain a continuous exchange of information between all the federal security authorities as a basis for effectively averting dangers and actively preventing risks.

It was precisely this realisation that prompted the German government to set up the National Cyber Response Centre four years ago. The centre is a core component of the Cyber Security Strategy (CSS) formulated in 2011, which updated the previous National Plan for Information Infrastructure Protection from 2005, and adapted it in light of the increasing challenges of the new decade. The following federal authorities are represented in the National Cyber Response Centre under the leadership of the Federal Office for Information Security, where the new office is also located.

- Military Counter Intelligence Agency
- Federal Office of Civil Protection and Disaster Assistance
- Federal Office for Information Security
- Federal Office for the Protection of the Constitution
- Federal Criminal Police Office
- Federal Intelligence Service
- Federal Police
- Federal Armed Forces
- Customs Investigation Service

Special administrative agreements between the participating authorities provide the basis for these cooperative efforts to attain increased IT security. The agreements strictly respect the division of statutory responsibilities and respective powers of all the bodies involved. The principle of legality and the requirement for separation between the intelligence services and the police are particularly important here. Each authority appoints a contact person with individual responsibility as their staff member at the Cyber Response Centre, which is managed by the Federal Office for Information Security representative. The president of the Federal Office for Information Security is the spokesman for the Cyber Response Centre and thus its most senior representative.



Nationales Cyber-Abwehrzentrum

Particularly useful are the various synergies that result from the regular transfer of knowledge within the Cyber Response Centre.

A full picture of the situation with informed recommendations for action

The Cyber Response Centre's key tool is its daily review of the security situation. Recent incidents and findings from the participating bodies are raised, which are then referred to specialist teams of experts for a more detailed examination depending on the urgency of the issue. A technical analysis of the security incidents improves the overall picture of the current situation and also enables concrete recommendations for action to be formulated, which are directed at the relevant political and operational organisations and also at the National Cyber Security Council.

To further improve the picture of the IT security situation, the Cyber Security Strategy proposes increased involvement by operators of critical infrastructures, or KRITIS for short. KRITIS refers to organisations with major importance for the public good, such as water or electricity suppliers. The computer systems of these organisations are particularly vulnerable because a severe loss of function – or even complete failure in a worst case scenario – could lead to supply shortages or significant disruption to public safety. By participating in the Cyber Response Centre, the representatives of the KRITIS organisations enable additional information from different sectors to be incorporated into the overall picture of the situation, thus enabling broader and more in-depth recommendations to be formulated.

It should be emphasised that although the participating authorities and institutions work together in close cooperation in the Cyber Response Centre, they carry out all operational tasks within their own remit and according to their individual areas of responsibility. However, their work is aided by the diversity of synergies that result, in particular from the regular transfer of knowledge within the Cyber Response Centre.
In the four years of its existence, the Cyber Response Centre has subjected its organisational structure, its working priorities and its cooperation models to continuous development. In doing so, it has successfully transformed from a simple information hub to a central cooperation platform for institutions with responsibility for IT security in Germany. ■

- **Federal Office of Civil Protection and Disaster Assistance**
- **Federal Office for the Protection of the Constitution**
- **Federal Office for Information Security**
- **Military Counter Intelligence Agency**
- **Customs Investigation Service**
- **Federal Criminal Police Office**
- **Federal Intelligence Service**
- **Federal Armed Forces**
- **Federal Police**

The cyber security summit

A look behind the scenes of the G7 conference

At the beginning of June, German Federal Chancellor Angela Merkel invited six heads of state and government of the G7 nations – Russia was excluded for political reasons – to a summit at Schloss Elmau in Bavaria. This mammoth organisational task posed a huge challenge for security experts in particular. In addition to physical security, it was essential to protect the conference against cyber security attacks. Successful cooperation between all the parties involved ultimately turned Schloss Elmau into a cyber maximum security unit for two days in which the heads of government were able to discuss global issues undisturbed.

Images of the protests at the opening of the new ECB headquarters in Frankfurt were still very fresh in the mind when the G7 summit began in June – but in addition to physical risks, threats to IT security took on an increasingly important role at Schloss Elmau. It was crucial to safeguard the on-site networks for the delegations and for more than 5,000 journalists who had travelled to Bavaria, and also to secure the various websites that provided information about the summit. Protection was also required for the networks and websites belonging to the authorities involved in supporting the summit and other authorities of the federal administration. These networks and sites represented potential targets of opportunity for cyber criminals.

In addition, activities were coordinated with the regional authorities, the police and also the regional CERTs within the German government's CERT group. Information on threats and protection measures was shared and discussed very early on.

Highly critical risk assessment

Following a number of larger IT security incidents prior to the conference, the cyber threat level was raised to high and thus was incorporated in the National Situation Report produced by the Federal Criminal Police Office and the Federal Ministry of the Interior. At the beginning of 2015, Distributed Denial of Service (DDoS) attacks had paralysed German government websites shortly before the Ukrainian prime minister visited Germany. Then – following the shootings at the offices of French satirical magazine Charlie Hebdo and subsequent mass website defacements in Germany that were attributed to Islamic sources – the French TV channel TV5 was severely disrupted by hackers and the German Bundestag suffered an espionage attack during the summit. These hacktivist attacks inside and outside Germany, believed to be politically motivated, were regarded as a major threat.

Besides one-off campaigns like these, there is also the ongoing risk of conventional espionage that aims to uncover the negotiating positions of the various delegations and sherpas, or gain information on outcome documents early on in the proceedings. Criminals could also have taken advantage of the highly newsworthy summit to launch spam and phishing attacks. Important political events are always potential targets for terrorists who use attacks to attract attention and spread fear, both online and offline.

Cooperative defence

For this reason, the federal administration and other parties involved were made aware of protection measures prior to the conference, particularly in relation to their external interfaces. At major events like this, it is essential to improve communications between the various public authority representatives, such as IT security officers, PR managers, website designers and hosting providers. Here, an approach has proved effective whereby the participants involved discuss the different possibilities of attack. It is important to have addressed IT security aspects before contracts are drafted and awarded. The availability of websites and the integrity of their content need to have been secured against defacement or malware distribution by the operational stage at the latest.

For particularly vulnerable websites, penetration testing was conducted by the Federal Office for Information Security in order to identify potential weaknesses and remedy them as quickly as possible. All authorities were requested to review their DDoS protection and make the necessary arrangements with their hosting providers. This is the only way to guarantee a rapid and well-planned response in the event of an attack. In this context, responses should also be planned for situations in which the usual protection mechanisms are no longer adequate because of excessive bandwidth, and that action needs to be taken at higher network levels.

Important political events are always potential targets for attracting attention or spreading fear.

Counter surveillance: beware, walls have ears

A significant part of securing the summit by the Federal Office for Information Security was carried out by counter surveillance colleagues. They checked the rooms for hidden listening devices prior to the conference and monitored the frequency spectrum throughout the event for anomalies that could have indicated eavesdropping attacks. The motto "Keeping confidential matters confidential" provided the backdrop to all the preparatory work and measures adopted by the counter surveillance team at the G7 meeting in Elmau.

A positive conclusion: no unusual incidents

The various events held in advance of the summit, including meetings of different ministers, proceeded without incident for the Federal Office for Information Security. The summit itself was not affected by some smaller attacks that took place. A DDoS attack on summit websites was stopped, while intrusive disruption in parts of the network used by the press was remedied within a short time. The Federal Office for Information Security kept forces on standby in the background around the clock in order to monitor the government's IT infrastructure and be ready to act in the event of larger attacks. ■

Stefan Ritter, Head of Situation Centre and CERT-Bund for IT security measures at the Federal Office for Information Security

Ensuring confidential information remains confidential

The content of political discussions is not intended for external audiences. If confidential information should come into the possession of individuals with criminal – or even terrorist – intentions, the security of an entire country could, in certain circumstances be placed at risk. That is why eavesdropping countermeasures, have the highest priority at events such as the G7 summit. The Federal Office for Information Security has both the necessary technology and the requisite expertise to ensure that politicians are able to engage in discussions without fear of being eavesdropped upon. The conclusion was that no illegal eavesdropping attack was detected.

Eight questions and answers about the Federal Office for Information Security's eavesdropping countermeasures at the G7 summit in Elmau.

1. Why are eavesdropping countermeasures so important at an event like the G7 summit?

In its role as current president of the G7 group, Germany hosted this year's summit in the Bavarian town of Elmau. A crucial aspect of such meetings is to ensure that conversations held in confidential settings remain confidential, and the information discussed does not find its way into the hands of unauthorised individuals. The Federal Office for Information Security's Eavesdropping Countermeasures section was therefore on hand in Elmau to protect the event against eavesdropping.

Volker Fricke, head of section, Eavesdropping Countermeasures

2. What role did the Federal Office for Information Security play at the event?

Preparations for the event began several months in advance when the German Federal Foreign Office, as the organiser of the summit, was advised by the Federal Office for Information Security on which technical and organisational measures would be needed for confidentiality and which should be avoided.

3. What are the biggest areas of weakness for eavesdropping attacks?

Interpreting facilities are normally constructed at international events so that discussions can be translated into all the participants' native languages. In this context, problems can be caused by interpreting facilities that communicate discussion content by means of invisible infrared beams. These beams can penetrate conference room windows virtually undiminished, meaning that with relatively little effort discussions can be eavesdropped upon from outside, even from some distance away. Therefore, only cabled-based interpreting equipment was used at the G7 summit.

The GSM bug provides the functionality of a mobile phone in a very small space in order to listen in to background conversations.

4. What potential risks are associated with participants' mobile devices?

Another vulnerability can arise when participants bring mobile devices (e.g. smartphones, tablets) into confidential meetings. We cannot completely eliminate the possibility of malware which could record the content of discussions and transmit it to unauthorised parties. The Federal Office for Information Security therefore offers the use of a mobile communications detection system which recognises and locates unwanted devices.

5. What specific tasks did the Federal Office for Information Security undertake on site?

The work of the Eavesdropping Countermeasures team on the ground essentially consisted of two components: inspecting vulnerable rooms for hidden eavesdropping equipment and continuously monitoring the high frequency spectrum for anomalies which could indicate active listening devices.

6. How were the rooms prepared in advance of the meeting to ensure they were protected against eavesdropping?

Inspections of all rooms were carried out, including the conference rooms and areas intended for confidential bilateral talks. These inspections began simultaneously with the furnishing of the conference rooms because it required the closing up of hollow spaces and cavities which could be used to conceal eavesdropping devices. In addition to visual checks, the rooms were also inspected with special counter eavesdropping equipment. This also included technical infrastructure, i.e. lighting and wiring. High frequency receivers and antennas were also installed during the furnishing. Ideally, this took place as close as possible to the conference proceedings in order to facilitate tracking of suspicious signals.

7. How did you manage to install the security technology so inconspicuously that the summit participants were still able to hold talks in a relaxed atmosphere?

In Elmau, the conference tables had a large hollow cavity in the base which provided enough space for our technical equipment. The receivers were controlled via a fast IP computer network, allowing an existing network infrastructure to be used. Processing and evaluating the recorded data could therefore be carried out centrally where the main interpreter control point and interpreting booths were located.

A concealed camera built into the clock records images and sounds from the surrounding area.

8. How did the background technology operate?

A recording vehicle belonging to the Federal Office for Information Security was parked outside near the conference rooms. The vehicle contained a further high frequency receiver and a powerful direction finder. This equipment made it possible to detect unusually high frequency signals, both in advance and during the meetings, which could have indicated an illegal eavesdropping attack. The signals were compared with the readings from the conference rooms and evaluated to determine whether the signals originated from within the conference rooms or outside. ■

The IT Security Act

Steve Ritter and Dr Timo Hauschild discuss the new tasks for the Federal Office for Information Security

The IT Security Act came into force at the end of July after lengthy preparations and lots of discussion. What is changing?

Steve Ritter: The IT Security Act will bring lots of changes, both for the Federal Office for Information Security and for industry. The Federal Office for Information Security has received a clear mandate from legislators to focus its work much more intensively than before on increasing the security of the federal administration's IT systems. The intention is for the Federal Office for Information Security to step up the development of minimum standards that all federal authorities should implement, or – after validation by the Ministry of the Interior – must implement.

In future, the Federal Office for Information Security will also play a major role outside the federal administration and this will be particularly apparent in relation to critical infrastructures. In the future, the Federal Office for Information Security will support critical infrastructure operators – either directly or via qualified service providers – and will increase the amount of information it currently supplies to them. This will enable the operators to improve the protection of their IT systems. As well as acting as a central reporting office for the federal administration, the Federal Office for Information Security will also become a a central contact point for critical infrastructure operators.

Critical infrastructure operators will receive information from the Federal Office for Information Security and will also be required to notify the Federal Office of significant IT security incidents so that other operators can be promptly warned of attacks.

Timo Hauschild: What is even more important, however, is the requirement for critical infrastructure operators to secure their IT systems using state-of-the-art security measures and provide evidence by way of regular checks to show that these security measures are being implemented. This is because nowadays virtually all critical infrastructures, such as the water supply or food production sectors,

The greater the number of people who are supplied by a facility with a critical service, the more important it is for this facility not to fail.

Steve Ritter, specialist advisor in the IT Security and Law section

Dr Timo Hauschild, head of section, Critical Infrastructure Protection (CIP)

are dependent on fully functioning IT systems. Therefore, it is crucial to secure not only the infrastructures themselves, but also the relevant IT systems if we don't suddenly want to be left high and dry one day because a hacker has attacked a water supply company's computer system.

The drawing up of the security measures is largely left up to the operators themselves. However, for energy networks, power plants and public communications networks, specific guidelines are published in a series of catalogues by the Federal Network Agency. These build on the guidelines that were in place before the IT Security Act came into force.

Obligations for website operators and hosting providers

In accordance with section 13 sub-section 7 of the German Telemedia Act (TMG), service providers offering telemedia services on a commercial basis will be obliged to improve the protection of their IT facilities. Service providers are, for example, website operators and their web hosting providers. Where it is technically and economically reasonable, they must employ state-of-the-art technical measures to stop unauthorised attacks on their systems and on personal data, and to prevent malfunctioning (e.g. due to attacks).

The Federal Office for Information Security has observed that one of the most common security errors is the failure to apply updates and security patches. This makes it easier for attackers and others to use the website to spread malware to its visitors.

Note: This obligation applies only to commercial websites; private websites or websites for clubs and associations will not normally be affected by this. However, a website may be deemed to be commercial if revenue is generated through it, e.g. from advertising.

What is actually happening now?

SR: The reporting and security obligations do not apply to everyone at the same time. The holders of nuclear licences already need to report IT security incidents to the Federal Office for Information Security. Operators of public telecommunications networks and services must also immediately meet the tighter security and reporting obligations in accordance with the Telecommunications Act (TKG).

However, there is a grace period for most critical infrastructure operators because what determines a critical infrastructure within the meaning of the Act on the Federal Office for Information Security can only be defined within statutory ordinance. The corresponding obligations cannot have an effect before that.

	Duty to implement state-of-the-art IT security measures	Duty to check security measures (e.g. in audits)	Prompt provision of relevant information by the Federal Office for Information Security	Duty to report IT security incidents	Advice and support options provided by the Federal Office for Information Security
KRITIS operators in accordance with Federal Office for Information Security KRITIS regulation (apart from special cases, see the three following rows).	Yes. Specifically defined within industries. Two years after regulation enters into force at the latest.	Yes. Verification and evidence every two years. First time must be two years after regulation enters into force.	Yes.	Yes. Six months after regulation enters into force at the latest.	Yes.
Public telecommunications networks in accordance with Federal Office for Information Security KRITIS regulation.	Yes. Specifically defined using IT security catalogue in accordance with section 109 of the Telecommunications Act (TKG) (former regulation).	BNetzA checks implementation every two years.	Yes.	Yes, immediately. Duty to report to BNetzA (extension of former regulation).	Yes.
Public telecommunications networks (other operators).	Yes. Specifically defined using IT security catalogue in accordance with section 109 of the Telecommunications Act (TKG) (former regulation).	BNetzA checks implementation every two years	No.	Yes, immediately. Duty to report to BNetzA (extension of former regulation).	No.
Energy supplier networks in accordance with Federal Office for Information Security KRITIS regulation.	Yes. Specifically defined using IT security catalogue in accordance with section 11 (1a) of the Energy Act (EnWG) (extension of former regulation).	Yes. Specifically defined using IT security catalogue in accordance with section 11 (1a) of the Energy Act (EnWG).	Yes.	Yes. When regulation enters into force.	Yes.
Energy supplier networks (other operators).	Yes. Specifically defined using IT security catalogue in accordance with section 11 (1a) of the Energy Act (EnWG) (extension of former regulation).	Yes. Specifically defined using IT security catalogue in accordance with section 11 (1a) of the Energy Act (EnWG).	No.	No.	No.
Energy plants in accordance with Federal Office for Information Security KRITIS regulation.	Yes. Specifically defined using IT security catalogue in accordance with section 11 (1b) of the Energy Act (EnWG).	Yes. Specifically defined using IT security catalogue in accordance with section 11 (1b) of the Energy Act (EnWG).	Yes.	Yes. When regulation enters into force.	Yes.
Licence holder in accordance with sections 6, 7 or 9 of the Atomic Energy Act (e.g. nuclear power plants, nuclear repositories).	Yes. (No change to the existing Atomic Energy Act).	Yes. (No change to the existing Atomic Energy Act).	Yes.	Yes (since 25 July 2015).	No. Unless they are KRITIS operators.

The IT Security Act introduces five new duties and tasks for KRITIS operators. The table shows which duties and tasks apply to which operators, when and how.

> *Operators of critical infrastructures will be able to improve the protection of their IT systems. As well as acting as a central reporting office for the federal administration, the Federal Office for Information Security will also become a central agency for critical infrastructure operators.*

→ **TH:** The Ministry of the Interior is currently working with us and with other relevant ministries, regulators and industry representatives on the question of which operators are covered by the new provisions contained in the Act on the Federal Office for Information Security. This will be regulated as part of the Federal Office's critical infrastructures (KRITIS) regulation. The regulation will be developed in two parts: the first for the energy, ICT, food and water sectors, and the second for transport and traffic, finance and health.

Once the regulation becomes effective, the operators concerned have two years in which to implement state-of-the-art security measures for their IT systems and provide evidence of them to the Federal Office for Information Security. They must also nominate a contact person who will be responsible for notifying the Federal Office for Information Security and who will respond to any queries from the Federal Office. This must take place within six months of the regulation coming into force.

The Federal Office for Information Security is currently devoting a great deal of time and effort to preparing for its new responsibilities. But there is still much to be done. For example, the reporting criteria and notification channels need to be established. On top of this, a firm definition of "state-of-the-art" is required in relation to IT security. In order to ensure legal certainty here, the industries involved can develop industry-specific security standards and have their suitability approved by the Federal Office for Information Security.

Obligations on providers

Operators of public telecommunications networks (e.g. telecommunications companies) and providers of publicly accessible telecommunications services (e.g. email providers) will in future be required to report any significant security breaches of their networks or services to the Federal Network Agency (BNetzA). In particular, this includes incidents that could result in unauthorised access to the IT systems of their customers. The BNetzA may also inform the public if appropriate. Where IT security is affected, the BNetzA must notify the Federal Office for Information Security in every case. The BNetzA can oblige the network operator and service provider to implement security measures.

If a service provider becomes aware of faults within a user's IT system, it is required to inform the user of these faults. However, this duty only applies where the user is already known to the provider. To a reasonable extent, the provider is obliged to inform users about tools (e.g. anti-virus programs) which users themselves can deploy to detect and eliminate faults.

Will this all be regulated in statutory ordinance?

SR: That is often the expectation being heard. However, the regulations in a statutory ordinance may not go beyond the bounds of the framework specified in the respective Act. In the case of the IT Security Act, the Ministry of the Interior is only permitted to regulate which facilities, systems or parts of these are to be regarded as critical infrastructures within the meaning of the Act on the Federal Office for Information Security. The ordinance is thus not allowed to contain any regulations on reporting channels, notification thresholds, auditors or other matters.

TH: Exactly, the IT Security Act includes a few mandatory elements to supplement the cooperative approach that has been taken for several years with the Critical Infrastructures Protection Implementation Plan (UP KRITIS) project for the protection of critical infrastructures (an article on this entitled "Critical infrastructures" appeared in the Federal Office for Information Security magazine 2013/14). The formulation of the Act will be tackled cooperatively along the same lines. We have already begun to engage in intense discussions with the committees that are dealing with UP KRITIS with the aim of defining frameworks for industry-specific security standards. The same applies to implementing the reporting obligation and to the needs and wants of the operators with regard to information that will in future be issued by the Federal Office for Information Security.

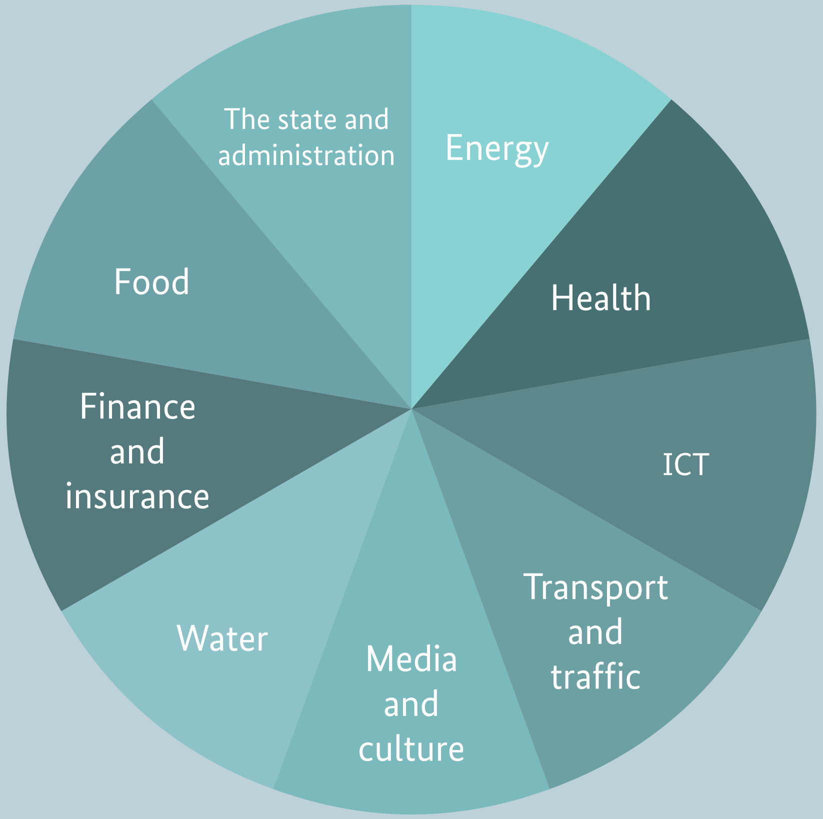
The KRITIS regulation developed by the Federal Office for Information Security regulates the "Who?". It will thus contain information on qualitative and quantitative criteria which the KRITIS operators can use to check whether the facilities they operate are critical infrastructures within the meaning of the Act. The qualitative criterion focuses on the delivery of a critical service. This type of service could, for example, be the supply of water, energy or food. The quantitative criteria contain threshold values, i.e. levels of supply; ultimately it's about the number of people actually or potentially being supplied by a facility. The focus is always on what the possible consequences would be for Germany's citizens if a facility were to fail. The greater the number of people who are supplied by a facility with a critical service, the more important it is for this facility not to fail.

→ The main changes brought about by the IT Security Act do not only concern critical infrastructure operators. What will change for Germany's citizens?

SR: Citizens will indirectly benefit from the regulations to protect critical infrastructures. It is hoped they will be spared the impact of shut downs, such as those that could affect energy or water supplies, but if these do happen, they won't have been caused by hacker attacks or IT security risks.

There is also a wide range of regulations that citizens will benefit from directly. For instance, telecommunications providers must now warn users if they notice that their IT systems are being misused, such as if they have become part of a botnet. Providers must also highlight suitable tools that users can use to identify what is causing a problem and remove it from their system. This means they no longer have to deal with things on their own, but can benefit from their telecommunications provider's expertise.

A far-reaching change that will bring benefits for citizens is the amendment to the Telemedia Act (TMG) which will oblige website operators and hosting providers to use state-of-the-art security in future to protect their IT systems from unauthorised attacks and disruptions. This is expected to make it more difficult for attackers to spread malware via reputable websites. These drive-by downloads, where the user becomes infected by malware simply by visiting a website, continue to be a major problem.



The critical infrastructures are divided into nine sectors.

Product inspections by the Federal Office for Information Security

Thorough inspections are necessary in order to ensure an IT product is free of any weak points. However, many inspection methods involving reverse engineering are currently associated with legal risks. The new section 7a of the Act on the Federal Office for Information Security (BSIG) empowers the Federal Office to inspect IT products so that it may fulfil its tasks with regard to the German government's requirement for the protection of critical infrastructures. If security flaws are discovered during these inspections, the public must be alerted if necessary, after first involving the manufacturer.

However, the inspections carried out by the Federal Office for Information Security are not designed to be consumer tests for IT products. Extensive test reports and comparisons of IT products can already be found in many specialist publications, and the Federal Office for Information Security will not compete with these.

Stealing citizens' personal data in web server attacks will also become much more difficult once the new security obligations are implemented. In the past, website operators often neglected to take even the simplest of measures, such as applying security patches, and therefore made data theft very easy for attackers. But hopefully this will now change, meaning citizens will be able to navigate the Internet much more safely.

That sounds like a lot of new changes. Will the Federal Office for Information Security be able to manage them all?

TH: The IT Security Act specifically aims to strengthen the Federal Office for Information Security. The new responsibilities mean new posts and thus new employees for the Federal Office for Information Security. Staff recruitment has already begun. The task now is to implement the new requirements in organisational terms, but a lot of what we need to do builds on or extends things that the Federal Office for Information Security has been doing for years. We are therefore confident that we will be able to handle our new responsibilities very well.

SR: I can only underline what Dr Hauschild has said. A major success factor here is that the relevant departments in the Federal Office for Information Security have worked together intensively and very effectively for many years. Without the successful teamwork of people from various disciplines, we would have had no chance of being able to repeatedly deal with such a dynamic issue. ■

Obligations on KRITIS operators The new BSIG regulations require critical infrastructure (KRITIS) operators to implement state-of-the-art security measures to prevent disruption to, or failure of, the IT systems, components and processes necessary for the proper functioning of the critical infrastructures they operate.

The operators must provide evidence on a regular basis – at least every two years – to the Federal Office for Information Security to show that state-of-the-art security measures are being implemented. The state-of-the-art can be defined specifically for an industry as part of an industry-specific security standard, which can be developed by the respective industries.

Furthermore, KRITIS operators covered by the Act are obliged to notify the Federal Office for Information Security of all significant security incidents, i.e. disruptions to the availability, integrity, authenticity and confidentiality of their IT systems that have, or may have, an impact on the operation of the critical infrastructures.

The Federal Office for Information Security is to become the central reporting office for operators of critical infrastructure in matters related to the security of information technology. It has been assigned the task of gathering and evaluating the information necessary to prevent threats to IT security, and is responsible for examining this information to ascertain the potential impact on the availability of critical infrastructures, create and maintain an overview of the current situation, and inform the KRITIS operators and the relevant (supervisory) authorities. The Act not only obliges KRITIS operators to provide reports to the Federal Office for Information Security, but also ensures they receive information, evaluations and recommendations in return. The Federal Office for Information Security can also provide support and advice to the KRITIS operators on IT security measures, or may refer them to appropriately qualified security providers. The Federal Office for Information Security's responsibility for the IT security of the federal administration is thus extended to include critical infrastructures.

The 14th German IT Security Congress in Bonn/Bad Godesberg

From May 19th to 21th 2015, representatives from the German IT security scene gathered in Bonn for the 14th time. Around 600 visitors from the worlds of politics, public administration and business met at the 14th German IT Security Congress in Bad Godesberg to discuss the current challenges involved in protecting IT systems and Internet communications.

The content of the keynote speeches, presentations and discussion sessions covered a wide range of different topics including secure mobile communication, IT security management, cloud computing and industrial security. Over the course of the congress, it became particularly clear that the ongoing digitisation of nearly all areas of life and work is creating new targets for cyber attacks. Those potentially affected are business, academia and state bodies, as well as citizens themselves. In this context, the general consensus among the congress visitors was that conventional security measures have reached their limits and that professional risk management should not concentrate solely on risk prevention, but should also increasingly integrate risk minimisation measures into procedures. However, this also implies as a consequence the requirement for improved options for an effective crisis response to successful attacks on networks and IT systems. "The hot topic is risk management," emphasised the president of the Federal Office for Information Security, Michael Hange. In his view, we need to learn to deal with uncertainty better because it cannot be completely eliminated in cyber space – no more than in other walks of life.

A plea against digital carelessness

At the very beginning of the congress, Federal Minister of the Interior Dr Thomas de Maizière referred to digital carelessness in his opening speech and called for greater individual responsibility where this was concerned, especially on the part of companies.

The rate of infection for computers has actually risen to an alarming degree over the past six months, as Markus Schaffrin, divisional manager of the eco Association of the German Internet Industry, explained in Bad Godesberg: "Our statistics prove that around 40 per cent of computers are infected with malware. And it is not only one security threat but ten on average that are found on computers."

Many companies were unaware that they had already been attacked, said Hartmut Isselhorst, head of the Cyber Security Department at the Federal Office for Information Security.

"I believe that this situation changes as soon as attacks are first experienced." However, "digital helplessness" then usually sets in, said the head of department. He said that the Federal Office for Information Security provides pragmatic support in the form of comprehensive information and services – both on the question of what needs to be done to provide a rapid response if required, and also on the prevention measures that lead to a sustained increase in IT security.

IT security needs to be made easy

It is essential to take IT security into consideration as early as the product development stage and incorporate it into the entire lifecycle of the product. Products need to be created and refined by users during development, as is the case with tablets and smartphones because only "security made easy" is really good security, according to the Minister of the Interior. This also means that users need to be confident that the functions and processes running in the background have been developed securely and that security loopholes are closed as soon as they are discovered.

The state shares responsibility

Despite new threat scenarios that are constantly emerging, citizens' expectations from the state have not changed significantly – they expect the state to provide a protective and protecting role for the Internet and to take a degree of responsibility for the Internet as infrastructure. "The state has joint responsibility to ensure that citizens can live freely and protecting in a way that they are not subjected to harm," said the Federal Minister.

Another focal point of the congress was the design of the IT Security Act which has now become effective. The Act allocates new responsibilities to the Federal Office for Information Security, making it a central point of contact for all questions relating to the IT security of those critical infrastructures that have exceptional importance for the community. (You can also read the article on the IT Security Act in this magazine.) ■

"I think a key aspect of this congress is the fact that, in Germany, the state provides intensive support for the IT security of its citizens and businesses."

Peter Hohl, CEO of SecuMedia Verlags GmbH

"We find ourselves in the midst of a fundamental change to the economic system. Digitisation is enabling connections that we have never seen before."

Dr Klaus Mittelbach, CEO of the German Electrical and Electronic Manufacturers' Association

"The state should also provide a protective and safeguarding role for the Internet and take a degree of responsibility for the Internet as infrastructure."

Dr Thomas de Maizière, Minister of the Interior

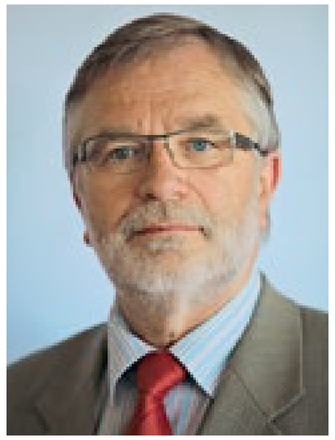
"Germany needs an IT Security Act so that critical infrastructures with major importance for the public good can be reliably protected from cyber threats. I consider a cooperative approach to the draft legislation to be especially important."

Michael Hange, president of the Federal Office for Information Security

Systematic estimation

How can IT security teams measure the cost and effort involved in implementing protection measures? A new aid for resource planning in IT security teams offers a solution.

A successful information security management system (ISMS) needs structure, organisation and staff. Data collection methods for quantifiable tasks cannot in all cases be used to determine staffing needs; estimated forecasts are then made instead. What level of staffing is appropriate for an IT security team? This question has led to lots of open-ended discussions in the past. The Federal Audit Office was involved in developing an estimation procedure for determining outlay and for planning the deployment of staff resources within IT security teams. This procedure has now become recognised as a solution and an aid which allows information security tasks, priority control and time requirements to be depicted in a transparent way. It describes the technical requirements for an effective ISMS and helps to determine minimum staffing levels.



Günther Ennen, head of section, IT Security Consulting for Public Authorities

Capabilities and limitations of the new aid

Empirical data for calculating the outlay required for IS team activities does not exist; therefore it is permissible and helpful to begin with estimates. Past empirical data from authorities serves as a basis for these estimates. The aid is in no way intended to be used to substantiate requirement requests for more staff. The information security tasks can often be managed through an internal reorganisation of existing staff. The criteria for estimating outlay have been selected so that they can be used for any authority. Specific features relating to individual authorities are therefore not depicted. However, the procedure described does not relieve an authority of the need to carry out an additional assessment of staffing requirements in accordance with the methods approved in the Manual for Organisational Reviews and Determining Staffing Requirements, after a consolidation phase.

Standard authority as a model

The aid is based on a model of a standard authority; deviations from the chosen standard are corrected on the basis of weighted value tables through proportional time bonuses and/or deductions with regard to expenditure.

The standard authority

- has approximately 500 employees
- has a homogeneous IT landscape
- operates IT systems and IT processes with a normal security need
- has no field offices
- has no requirements in terms of high availability of IT systems or applications

The responsibilities of the ISMS increasingly include risk assessment of current alerts, responses to current security recommendations, time-sensitive alerts, manufacturer security updates and patches, and daily reports on the information security situation. Tasks that are commonly the responsibility of IT operations, e.g. the testing, approval and release of software, involvement in the creation of test plans, or the evaluation of security products, also require input from the IS team. The aid is a moderate and practical approach that has already proved useful for many authorities. ■

The aid and the estimation tool are available to download free of charge from the following link: www.bsi.bund.de/Personalschaetzung

Further information on the Manual for Organisational Reviews and Determining Staffing Requirements is available online at www.orghandbuch.de

Using the Federal Office for Information Security's estimation tool

A report on the use of the Federal Office for Information Security's resource estimation tool when setting up an ISMS

The IT Planning Council has agreed the Guideline on Information Security in Public Administration. This mandatory document applies both to the Federal Government and to the German federal states. One of the measures to be implemented is the development of an information security management system (ISMS) in accordance with Federal Office for Information Security standards.

Background information:

What is the Information Security Guideline?

- Approved by the IT Planning Council in March 2013
- Attainment of a mandatory minimum level of security between the Federal Government and the German federal states with IT-based, multilevel cooperation
- Implementation measures include:
  - Activities to raise awareness of information security
  - Training sessions in the context of the administration's CERT network
  - Support for implementing the IT-Grundschutz
  - Introduction of an information security management system in accordance with targets from the Federal Office for Information Security
  - Implementation of uniform minimum standards in information security
  - Protection of public administration network infrastructures
  - Collaborative defence against attacks on the administration's IT systems

Starting point

In North Rhine-Westphalia (NRW), an inter-departmental working group (WG) determined the implementation cost involved in introducing an ISMS according to the framework conditions specified by the IT Planning Council. The WG identified the key authorities concerned and produced a survey on the actual status of information security in the North Rhine-Westphalia state government.

Procedure

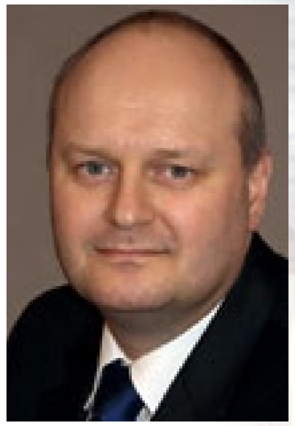
A comprehensive, authority-focused resource estimate was produced from these individual responses with the help of an external service provider and using the Federal Office for Information Security's estimation tool. Where no detailed information was available, plausible assumptions were made. At the same time, the posts already occupied were recorded.

Results and impact

The results, particularly the calculated staff and material expenditure, were incorporated into budget discussions. The draft budget was agreed by the state government in the meantime. Following the approval of the budget by the NRW state parliament, resources were made available for the development of an ISMS.

The estimation tool provided by the Federal Office for Information Security played a substantial part in ensuring the objectivity of the discussions on the often contentious issue of estimating expenditure. ■

Helmut Nehrenheim, specialist advisor in the North Rhine-Westphalia Ministry of the Interior and Municipal Affairs



Dr Frank Laicher, specialist advisor in the North Rhine-Westphalia Ministry of the Interior and Municipal Affairs

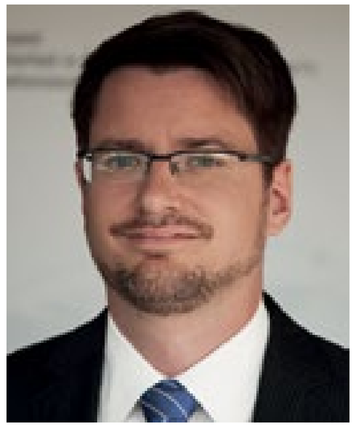
Trends such as cloud computing, Industry 4.0 and BYOD (bring your own device) create new security challenges and these are taken into account in the IT-Grundschutz.

Federal Office for Information Security modernises its IT-Grundschutz

Helping people to help themselves

The IT-Grundschutz produced by the Federal Office for Information Security provides public bodies and companies with an extensive compendium of IT security requirements and recommendations for implementation. This comprehensive standard work has become vast given the dynamic threat situation and pace of technological development. Reason enough, then, to modernise it thoroughly and bring it more closely into line with the day-to-day practice of IT users.

Germany is perhaps the only place in the world where such an extensive pool of methods and measures for the protection of information, IT systems and networks has evolved over more than two decades. The IT-Grundschutz was originally designed as a standard reference work with the primary aim of providing public administrative bodies with a well-founded system for identifying various security risks, along with recommendations for action. However, the private sector was also quick to make use of the IT-Grundschutz because it offers a pragmatic approach towards establishing individual protection needs and become effective internal IT environments. It is pragmatic in that it involves a continually developing process of collecting information and methods instead of a time-consuming and costly risk assessment of separate hazard classes for different systems and applications according to operational area. This eliminates the need for a detailed estimate of the probability of occurrence together with an assessment of the respective amount of damage. The IT-Grundschutz thus enables an adequate level of security to be implemented in a way that is economically feasible, even without extensive IT security expertise.



Holger Schildt, specialist advisor in the IT-Grundschutz and Alliance for Cyber Security section

Removing complexity

The Federal Office for Information Security works closely with industry to continually update the IT-Grundschutz in light of constant new cyber threats. Trends such as cloud computing, Industry 4.0 and the increased use of smartphones and tablets for a mixture of private and work-related purposes create new security challenges, and obviously these need to be taken into account in the IT-Grundschutz. The Federal Office for Information Security's standards and the IT-Grundschutz catalogues, plus handouts and recommendations, now amount to around 5,000 pages. The IT-Grundschutz's greatest advantage – its unique level of detail – has become a problem in itself: the enormity of it is intimidating and may scare people off. Many people feel overwhelmed by the sheer volume of information presented in it. On the other hand, they know that the IT-Grundschutz would be of little use if it did not refer to current dangers or contain concrete security recommendations. So what can be done? As a way out of this dilemma, the Federal Office for Information Security decided to thoroughly modernise the IT-Grundschutz to combine the need for a comprehensive standard work with the legitimate demand for greater ease of use.

Distinguishing between requirements and implementation

This will be possible by overhauling the fundamental modules which, unlike previously, will summarise the individual requirements in condensed form on a maximum of 10 pages without further implementation recommendations. This has the advantage of making the information easier to read and it also reduces the effort involved in producing the IT-Grundschutz modules. In the future, this approach will enable the Federal Office for Information Security to respond much more quickly to current developments in its creation of new modules. The finer detail will be separated out as implementation advice prepared for specific target audiences, such as IT administrators or in-house technicians. Thus the often daunting complexity of the earlier modules is removed. By distinguishing between requirements and implementation advice, the Federal Office for Information Security can tailor the necessary information precisely to the needs of individual roles in companies and organisations of all kinds. That means an IT officer will normally not require any extensive knowledge about how to implement the requirements in detail. The modernised modules save users time and effort, which in turn improves the chances of the IT-Grundschutz becoming accepted in Germany as a whole.

The requirements of these modules will be divided into three categories in future: basic, standard and high-level requirements for protection. Priority should be given to implementing the basic requirements as they achieve the maximum benefit with the least effort. Based on this, the standard requirements round out the state-of-the-art technology and address normal protection needs. In addition, the IT-Grundschutz catalogues offer suggestions for high-level protection measures. The Federal Office for Information Security is not only modernising the modules themselves, but also the layers into which the modules fit within the architecture of the IT-Grundschutz. The previous layers of Common Aspects, Infrastructure, IT Systems, Networks and Applications will be replaced by a new model: the IT modules will be divided into process and system-oriented groups in future. Process-oriented modules are those concerning common aspects, e.g. concepts, regulations or IT operations, such as patch management. Applications, IT systems and infrastructure are classed as system-oriented. Newly added are modules for industrial control systems, as greater emphasis is given to their protection in the modernised IT-Grundschutz.

Flexible entry versions and practice-based profiles

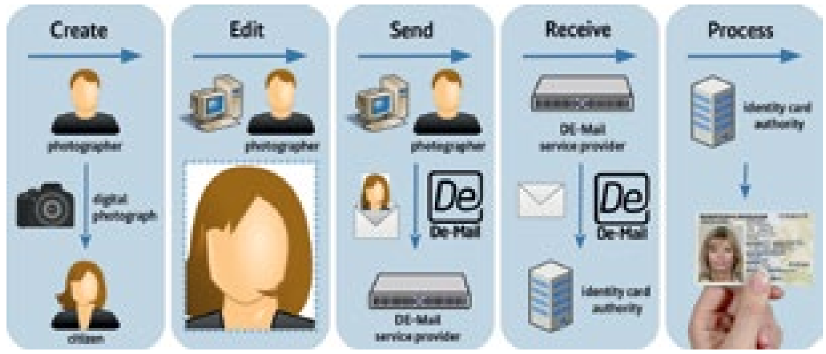
Moreover, the Federal Office for Information Security is breaking new ground by taking an approach to facilitate organisations getting started with the IT-Grundschutz. Experience has shown that the existing sequence of operations – in which a structural analysis, an assessment of protection requirements with modelling and a basic security check were carried out – was seen as a huge obstacle, especially by SMEs. Protective measures also took effect at a relatively late stage, with the institution concerned remaining vulnerable to various risks. It may therefore be appropriate to deviate from the previous IT-Grundschutz methodology initially, depending on which protection have already been implemented in an establishment. At the initial stage an institution could, for example, implement all basic requirements across the board in order to minimise the majority of risks as quickly and efficiently as possible. The detailed protection requirements analysis would then take place at a later stage using another procedure. In other cases, however, it may be useful to concentrate on protecting crucial data in the institution right from the start in order to ensure that those valuables that are particularly worth protecting are taken care of first of all.

Another key area of the modernisation project is the redevelopment of the IT-Grundschutz profiles. The basic concept of profiles is already in place in the standard IT-Grundschutz – in the form of example security concepts that demonstrate how a security concept can be planned, implemented and maintained for small, medium or large information networks. The new profiles should also be regarded as templates that can be used immediately by different groups of users to adapt the IT-Grundschutz to their own particular needs. Development of the new profiles may be undertaken in practice by users themselves in cooperation with the Federal Office for Information Security – with a clear focus on tailoring profiles to the specific industry or target audience. For instance, it would be conceivable for employees in law firms or medical practices to define which recommendations are essential, which are optional and which are unnecessary. In this way, the IT-Grundschutz profiles are developed by the target audience for the target audience. The new approach to the profiles is not only interesting for smaller institutions but also for local authorities, hospitals and even operators of critical infrastructure, such as those in the utilities sector. By focusing on practice and the model-nature of the new profiles helps institutions of all sizes save effort, time and costs in the implementation of their own personal IT-Grundschutz. ■

Secure, efficient and citizen-centred

De-Mail in public administration

E-mail has proved highly successful. It is widely used and very popular among the business community and the general public alike. This fast and convenient form of communication is also an integral part of Germany's public administration system. But e-mail also has its downsides. There is still room for improvement in confidentiality, integrity and authenticity. The advice of IT security experts to encrypt at least those e-mails with important or confidential content is rarely heeded – mainly because most users feel that the existing encryption methods are too complicated and thus not practical for everyday use.



The Federal Office for Information Security guideline on transmitting images via De-Mail for the issue of statutory documents has been available for all local government administrations since autumn 2014

Authenticity refers to the assurance that the alleged and apparent sender of an e-mail is the actual sender.

Integrity refers to the protection of the content of an e-mail, ensuring it remains unchanged during transmission.

Confidentiality refers to the guarantee that an e-mail and its contents can only be accessed by the intended group of recipients.

De-Mail, on the other hand, promises to gain wider acceptance because this procedure achieves greater IT security in a different way: De-Mail makes use of a closed communication network into which only those providers who have been accredited by the Federal Office for Information Security are admitted. Unlike e-mail providers on the Internet, De-Mail providers must successfully complete an extensive verification process according to clearly defined criteria in order to be accepted into the De-Mail network. The basis for this approach is the De-Mail Act and associated technical guidelines produced by the Federal Office for Information Security. Encrypted channels ensure the confidential transmission and integrity of De-Mail, while authenticity is guaranteed by the positive identification of all communication partners in the network. However, De-Mail does not intend to replace the conventional e-mail infrastructure completely. Rather, the objective of the procedure is to offer the traditional advantages of e-mail but with a demonstrably higher IT security level for specific tasks.

Introduction is well under way

The Federal government laid the foundation for De-Mail in April 2011 with the adoption of the De-Mail Act. In the following two years, four De-Mail service providers were accredited by the Federal Office for Information Security and now provide De-Mail services within Germany. These four existing providers are 1&1 De-Mail GmbH, Mentana-Claimsoft, Telekom Deutschland and T-Systems International.

The entry into force of the E-Government Act two years ago opened up new application areas for De-Mail. Since then, legally binding communication in written form can be replaced with De-Mail in certain circumstances. The Act also obliges the federal authorities to offer citizens and businesses De-Mail access for the transmission of electronic documents by spring 2016 at the latest. The German government has provided a central De-Mail link for its subordinate authorities since March 2015. One advantage of this federal gateway is that it enables the e-mail systems of all federal authorities to be linked in a simplified procedure, which is to be implemented gradually by March 2016. Federal authority employees will then be able to send and receive secure De-Mails using their normal e-mail client without the need for any major changes. Convenience and ease of use are essential to ensure IT security solutions are widely accepted by users.

Fewer visits to government agencies, shorter waiting times

Communicating with government authorities via De-Mail brings noticeable time and cost savings for citizens and businesses. In many cases, it will become unnecessary to visit the authority in person or send documents by post.

In terms of administrative efficiency, connection to the De-Mail infrastructure offers further potential – for example, by integrating De-Mail into the specific procedures and document management systems of each authority. This allows all documents received to be processed seamlessly and efficiently before being filed electronically once the necessary procedures have been completed without any need for manual intervention.

A pilot project has already been launched in the cities of Cologne and Göttingen demonstrating how De-Mail integration could be used in the future. The project involves transferring images by De-Mail for the issue of ID cards. With the consent of the applicant, biometric passport photographs are taken by photographers who then send them immediately to the relevant issuing authority via De-Mail. It is no longer necessary to have the photo developed and then scanned in once again by the authorities. ■

Ingrid Grüning, specialist advisor in the Secure eID Applications section

Secure communication platform for the smart energy grid

Smart networking of the future energy system presents major challenges for Germany, but also offers huge opportunities and exciting prospects for stakeholders in the German energy market. Germany is leading the way in Europe in establishing a uniform level of security for the smart energy grid. The ongoing development of security standards for key system components of the smart energy grid mean complex tasks for the Federal Office for Information Security.

Smart information networks can efficiently link and balance energy generation and consumption. The key elements of these networks are smart metering systems which provide clear information on energy usage and also securely transmit metering data. In addition, the systems provide a platform for the control of electronic appliances and power generation units, thereby improving load and generation management in the distribution network. The central component of a smart metering system is the smart meter gateway – a communication unit with an integrated security module.

Government and industry are developing common security standards

It is essential to establish a binding framework for the manufacture and operation of smart metering systems in order to ensure that the new technology is trusted and accepted, especially as it involves the processing of personal data. On behalf of the Federal Ministry for Economic Affairs and Energy, the Federal Office for Information Security developed the requirements for reliable product components (smart meter gateway with integrated security module), for their secure IT operation (administration) and for a trustworthy communications infrastructure (SM-PKI – smart metering public key infrastructure).

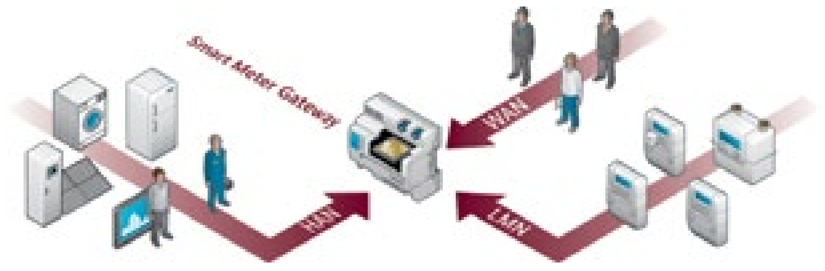
The development process included various organisations from the telecommunications, IT, energy, housing and consumer protection sectors, along with the Federal Commissioner for Data Protection and Freedom of Information, the Federal Network Agency and the Physical-Technical Federal Institute.

Smart meter gateway with integrated security module

The Federal Office for Information Security developed technical security standards in the form of two protection profiles, plus a technical guideline for the communication unit of a smart metering system (smart meter gateway with integrated security module).
A smart metering system thus consists of a smart meter gateway and one or more connected measuring devices (meters). Compliance with the technical security standards is verified by the Federal Office for Information Security as part of a certification process in accordance with Common Criteria (CC). Currently, eight smart meter gateway manufacturers, who have agreed to publication, are going through the CC certification process with the Federal Office for Information Security.

Protection of privacy by design

The protection of privacy was taken into account from the outset by involving the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in the development process. This was essential in order to prevent the creation of detailed user profiles which could potentially yield valuable information about the lifestyle habits of end customers. Evaluation profiles in the smart meter gateway can be designed to ensure that only the necessary consumption data relevant for billing is supplied for the various tariff profiles organised on a decentralised basis. This ensures the principles of data avoidance and data minimisation are observed.



The smart meter gateway as the communication unit in a smart metering system and as the central component between a wide area network (WAN), local metrological network (LMN) and home area network (HAN)

Guaranteeing the secure operation of smart metering systems

The smart meter gateway administrator is responsible for the secure technical operation of the smart metering system. It is therefore important to ensure that the IT operations of the administrator meet minimum requirements for the enforcement of information security. Currently, the requirements of the technical guideline include an information security management system check and an assessment of concrete security measures which extends beyond ISO 27001, using the IT-Grundschutz catalogues (the Federal Office for Information Security is the certification authority). In consultation with experts from the participating industry associations, the existing standards are currently being expanded with a further alternative that includes a test in accordance with ISO 27001 (native) and a package of measures to be implemented by the administrator. Certification in accordance with ISO 27001 (native) involves certification authorities that are accredited by Germany's National Accreditation Body (DAkkS) in accordance with IEC/ISO 27006 for information security management systems.

Dennis Laupichler, specialist advisor in the Industrial Cooperation and Standardisation section

Reliable communications infrastructure in a wide area network

The Federal Office for Information Security has root certification authority certificates for the SM-PKI. On the next level down are private companies, known as sub-CAs (subordinate certification authorities), which take over the issuing of end user certificates for the market participants.

The root is the central trust anchor of the smart metering system. In order to guarantee the protection of the transmitted metering data, mutual authentication of the communication partners is required to link the smart meter gateway with an authorised market participant in the wide area network. All communication takes place via an encrypted channel, the integrity of which has been secured. The technical, organisational and personnel-related security requirements for the issuing of certificates are defined by the root in a certification policy (root CP).

Since 1 March 2015, the live operation of the root has been carried out by a certification service provider under the supervision of the Federal Office for Information Security. In addition to the root, the market participants have been provided with various test systems for issuing digital test certificates in order to support the development and trialling of smart meter gateways and their associated components in field tests and pilots.

Continued development of security standards in the smart energy grid

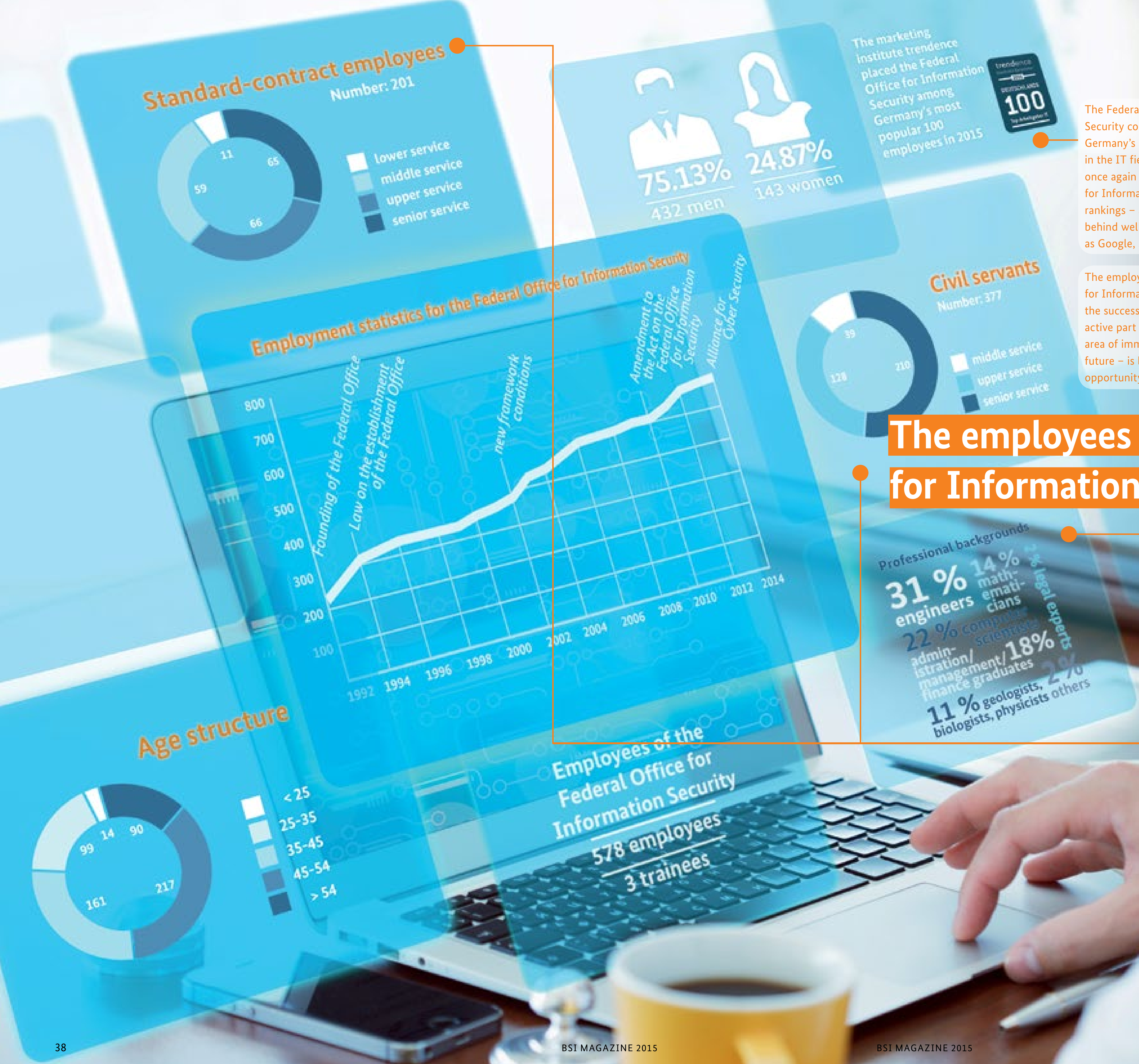
The protection profile for the smart meter gateway with its minimum requirements already provides the basis for establishing a uniform level of security in the smart energy grid. New and additional requirements have now been placed on the smart meter gateway and its associated components as a result of the various use scenarios and applications addressed in the key issues paper on smart grids which was published by the Federal Ministry for Economic Affairs and Energy on 9 February 2015.

In order to further develop the smart meter gateway as a secure communications platform for the smart energy grid, it is first of all essential to enable the secure communication of data on operating the grid and on power consumption and generation, as well as ensuring that load and generation management measures can take place securely. The capacity to measure other utilities (gas, water, heat) and the implementation of newly emerging value-added services, e.g. in the fields of building automation, smart homes and assisted living, must come next in future so that the full potential of a secure and standardised communications platform can be realised. The development of additional security and interoperability requirements for special applications (large gas metering stations, major electricity consumers, wind and solar parks) and the secure connection of decentralised components of the charging-station infrastructure follows, taking into account international standards. All of the departments, partner authorities, manufacturers and users who have participated to date must be involved in further development so that all parties concerned can also support and manage the targeted rollout of smart metering systems. The consultation procedure between the associations and the corresponding expert working groups of the Federal Office for Information Security proved successful during the development of the protection profiles and the technical guideline and will, therefore, continue as part of the ongoing development process.

Outlook on the legislative framework

In view of the regulatory material relating to fundamental rights and in order to avoid further fragmentation of energy legislation, it was necessary to combine all the regulatory subject matter in a new principal law. This serves to clarify procedures and also enables regulations to be determined beyond the law on the supply of electricity and gas (e.g. smart homes, district heat, thermal heat). The Federal Ministry for Economic Affairs and Energy aims to publish its Act on Digitisation of the Energy Transition in the second half of 2015 and, following a cabinet decision, present it to both the lower and upper house of the German parliament for approval and resolution. The new principal law on the operation of metering points and data communication in smart energy grids (Operation of Metering Points Act – MsbG) covers the setting of high technical standards (protection profiles and technical guideline) to guarantee data protection and data security, sector-specific data protection regulations for market communication, and also regulations relating to the installation and financing of smart meter systems. ■

More information online at: www.bsi.bund.de/SmartMeter



The employees of the Federal Office for Information Security

The Federal Office for Information Security continued to be among Germany's most popular employers in the IT field in 2015. IT graduates once again voted the Federal Office for Information Security into the rankings – at 16th place this year, just behind well-known companies such as Google, SAP, IBM and Microsoft.

The employees of the Federal Office for Information Security are vital to the success of its work. Playing an active part in shaping IT security – an area of immense importance for the future – is both a challenge and an opportunity.

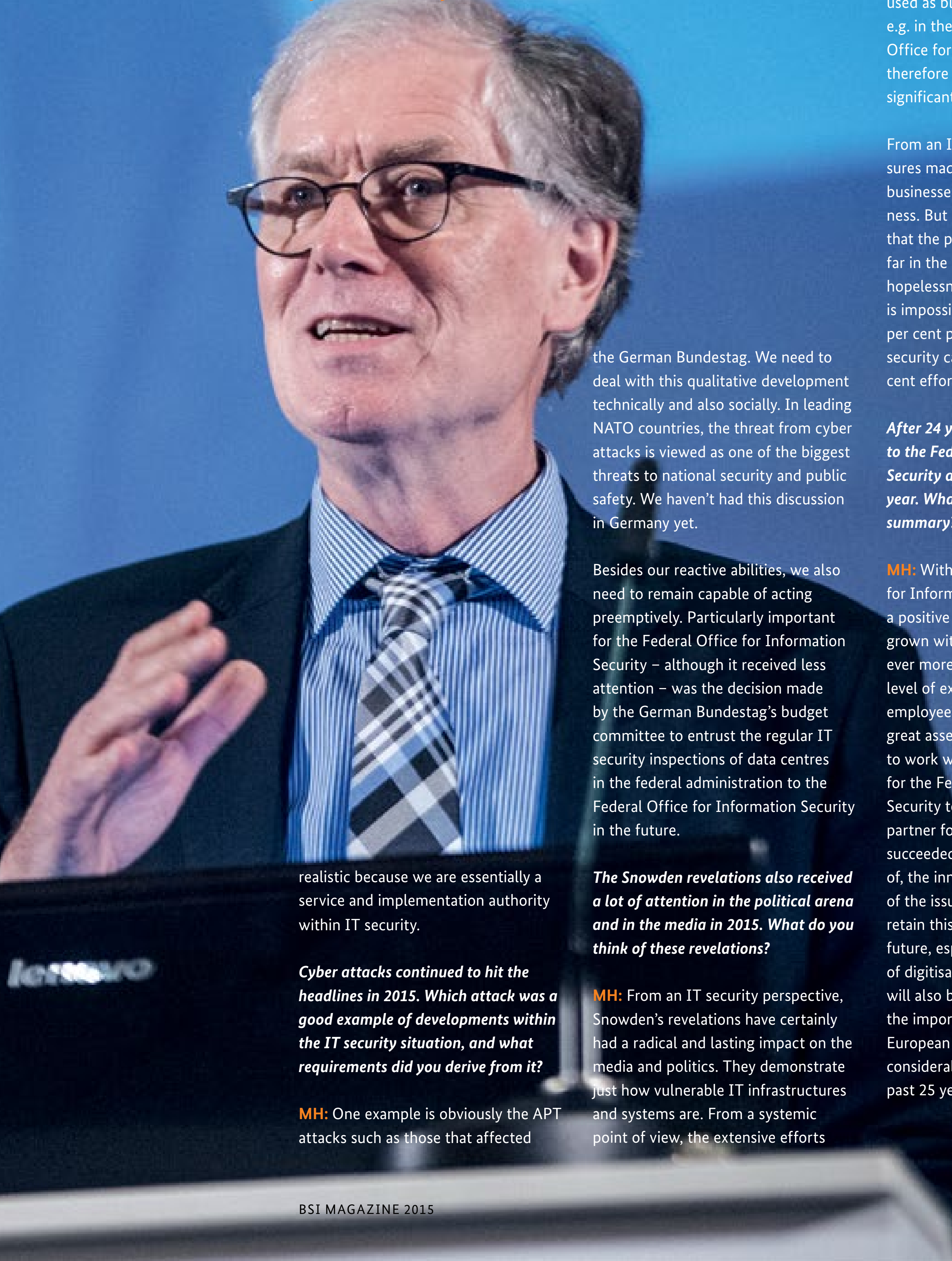
For the Federal Office's employees, providing IT security support in today's information society is not just a job, it is a vocation. In carrying out their duties, the Federal Office's employees are able to draw on a substantial knowledge base from a wide range of educational backgrounds including engineering, computer science, administration, management and finance.

The Federal Office for Information Security is committed to offering its skilled and dedicated employees all the opportunities available for the personal development of public service staff. Upgrading the skills of employees is included early on in strategic HR planning. The structure of the workforce at the Federal Office for Information Security is currently divided into 377 civil servants (Beamte) and 201 standard-contract employees. The actual breakdown of the different grades for civil servants and standard-contract employees contracts is shown in the diagram.

What has 2015 brought for IT security, and what will it bring?

Questions for Michael Hange, President of the Federal Office for Information Security

The interview was conducted by Joachim Gutmann, journalist from Hamburg



Mr Hange, what was the most significant event of 2015 for you with regard to IT security? What does this event mean for the Federal Office for Information Security?

Michael Hange: Without a doubt it was the enactment of the IT Security Act. It is a milestone because it is the first time the objective of working with operators to improve the protection of critical infrastructures has been set out legally. It takes into account the increasing threat posed by cyber attacks and uses more situation data from industry to formulate new strategies for defence – including the protection of members of the public.

The Act also reinforces the role of the Federal Office for Information Security as a central point for IT security matters for industry and society. The IT Security Act legally sets out what members of the public and industry already expect from the Federal Office for Information Security, which is not only the protection of the federal administration's IT systems, but also the provision of assistance for other users. We will meet these expectations

The Act allocates new duties and resources to the Federal Office for Information Security. Are these what you expected?

MH: The first part of that question is easy to answer. The German parliament assigned more responsibility to the Federal Office for Information Security by extending its existing operational remit: as a reporting office, in product testing, with regard to its alert functions and in the setting of standards in the federal administration. Its advisory role for business was also strengthened, and its capacity to influence standards of IT security was expanded. However, this also entails an obligation for the Federal Office for Information Security to meet its responsibilities and, when required, to offer practicable recommendations promptly. As a result, the Federal Office for Information Security's transformation process, which has been under way for some years, will continue, creating an operational authority with a focus on IT security.

And now for the second part of the question. The 50 posts granted for 2016 can only be a start in carrying out the tasks arising from the IT Security Act. More posts will be required to ensure these tasks are performed with skill and expertise in subsequent years, as IT security is the result of very dynamic and highly complex processes. If we want to keep pace with the attackers, we also need to be well equipped in terms of staff.

How flexible does the legal basis, on which the Federal Office for Information Security works, need to be in order to keep up with rapidly developing (technical) threats?

MH: We are continuously scrutinising our activities against new technical developments and the risk situation. New technologies and new business models, whose threat potential or safety gains need to be anticipated, represent a particular challenge here. We have been making this evaluation process transparent since 2014 in our annual status report for policy makers and the public. It provides the necessary flexibility both for the legal basis and also the cooperative approaches of the Federal Office for Information Security. However, the legislator must ultimately decide on the need for legislative action; I don't want to make any stipulations.

Is the integration of the Federal Office for Information Security into the structure of the Federal Ministry of the Interior the right thing for the new tasks, or should the Federal Office for Information Security be an independent authority?

MH: The issue of autonomy for the Federal Office for Information Security has in fact been raised in parliamentary circles and also in some sections of the media. We operate as an IT security provider for the entire federal administration by providing protection, alerts and advice. The Federal Office for Information Security also assists the federal authorities who perform monitoring tasks, such as the Federal Commissioner for Data Protection and Information Security. In addition, the Federal Office for Information Security assists other departments in matters of legislation relating to IT security (e.g. smart meters, healthcare cards) with more than 60 special statutory regulations. In the context of these responsibilities, I would wish for autonomy in the direct support of other ministries. However, I don't believe complete independence is realistic because we are essentially a service and implementation authority within IT security.

> "The IT Security Act legally sets out what members of the public and industry already expect from the Federal Office for Information Security, which is not only the safeguarding of the federal administration's IT systems, but also the provision of assistance for other users."

Cyber attacks continued to hit the headlines in 2015. Which attack was a good example of developments within the IT security situation, and what requirements did you derive from it?

MH: One example is obviously the APT attacks such as those that affected the German Bundestag. We need to deal with this qualitative development technically and also socially. In leading NATO countries, the threat from cyber attacks is viewed as one of the biggest threats to national security and public safety. We haven't had this discussion in Germany yet.

Besides our reactive abilities, we also need to remain capable of acting preemptively. Particularly important for the Federal Office for Information Security – although it received less attention – was the decision made by the German Bundestag's budget committee to entrust the regular IT security inspections of data centres in the federal administration to the Federal Office for Information Security in the future.

The Snowden revelations also received a lot of attention in the political arena and in the media in 2015. What do you think of these revelations?

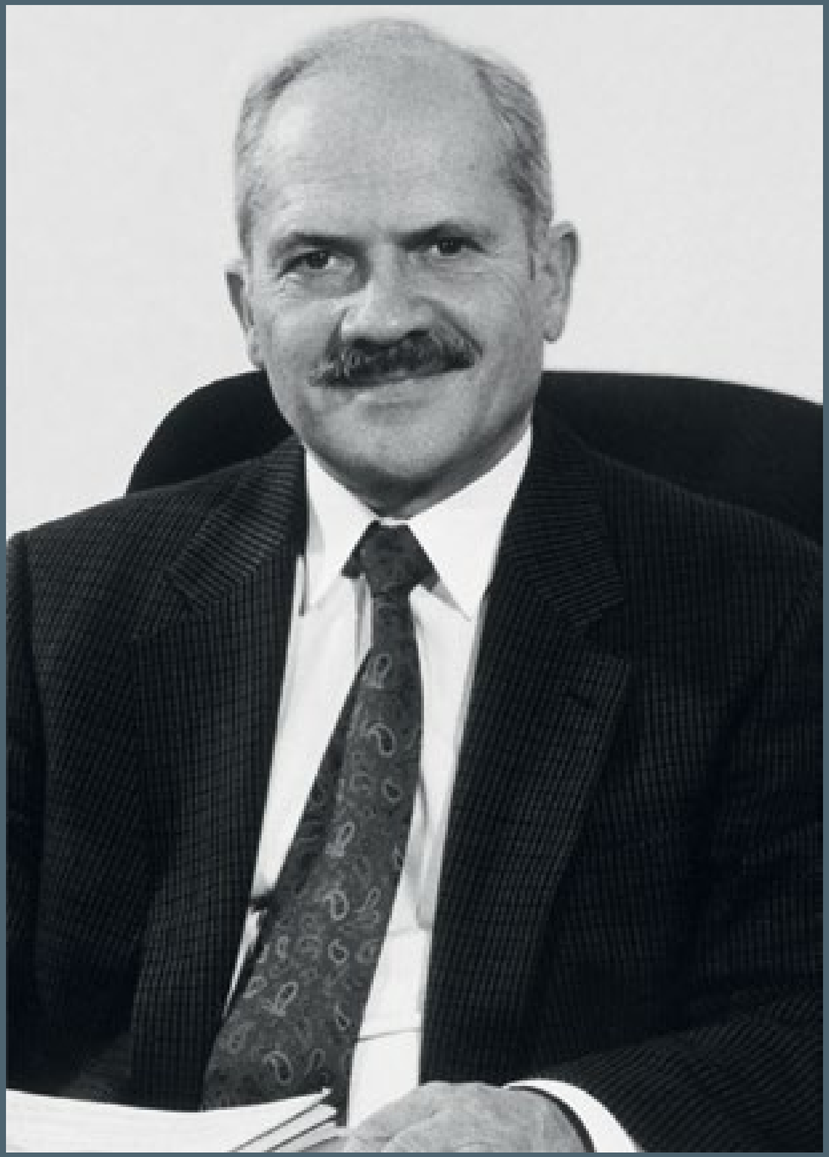
MH: From an IT security perspective, Snowden's revelations have certainly had a radical and lasting impact on the media and politics. They demonstrate just how vulnerable IT infrastructures and systems are. From a systemic point of view, the extensive efforts of intelligence services and also the indications of collaboration between US global players and the NSA even surprised the experts. But the fear is that some of the documents could be used as blueprints for copy-cat action, e.g. in the area of crime. The Federal Office for Information Security has therefore strengthened its analyses significantly in certain attack scenarios.

From an IT perspective, the disclosures made many citizens and many businesses face up to digital carelessness. But now we need to be careful that the pendulum doesn't swing too far in the other direction so that digital hopelessness takes its place. Even if it is impossible to achieve one hundred per cent protection, 80 to 90 per cent security can be achieved with 20 per cent effort.

After 24 years you are saying farewell to the Federal Office for Information Security and retiring at the end of this year. What would be your personal summary?

MH: With regard to the Federal Office for Information Security, it's definitely a positive summary. The agency has grown with the challenges and become ever more able to meet them. The high level of expert commitment shown by employees for IT security has been a great asset and it was very rewarding to work with them. My aim was and is for the Federal Office for Information Security to be recognised as an expert partner for IT security. I think we have succeeded despite, or perhaps because of, the innovative and dynamic nature of the issue of IT security. We must retain this flexibility and agility in the future, especially against the backdrop of digitisation. Proactive approaches will also be necessary in the future, as the importance of the German and the European ICT industry has narrowed considerably by comparison over the past 25 years. ■

Obituary for Dr Otto Leiberich
written by Michael Hange



Retired president Dr Otto Leiberich passed away on 23 June 2015 at the age of 87 after a short and serious illness.

As our founding president, Dr Leiberich continued to exert a pioneering influence on the Federal Office for Information Security (BSI) up to the present day. Through his vision and extraordinary commitment, he laid the foundation for the development and the future functions of the Federal Office for Information Security, building on the themes of cryptography and certification. In doing so, he contributed significantly towards helping the Federal Office acquire the public reputation that it enjoys today.

His outstanding professional achievement was establishing the Federal Office for Information Security in 1991. Dr Leiberich pursued this aim with dedication, perseverance and the ability to promote his ideas and convince others in the worlds of politics, business and academia. The core idea of his message was that a Federal Office for Information Security should go beyond protecting classified government information and be responsible for providing advice and assistance on IT security matters for all sectors of society. Looking back today, this was a very far-sighted approach that set the course for the future of the organisation, particularly in light of the importance of IT security today and its role in the digitisation of society as a whole.

Otto Leiberich also defined the strategic and operational focus of the Federal Office in its foundation phase, thus creating awareness of “start-up” opportunities.

Dr Leiberich retired in 1993 and continued his work on cryptology. In an article he wrote in 2000, which was highly regarded by experts, he said: “I have worked as a cryptologist myself for 45 years and have an overview of almost 100 years of cryptology thanks to contact with older colleagues.” In fact, Otto Leiberich is the chronicler of a huge shift in cryptology in Germany. He actively witnessed and helped to shape its development – from cryptography as a secret science to cryptography as one of the main pillars of present-day IT security.

Otto Leiberich was a passionate mathematician and cryptologist, and remained so even in retirement. Born in 1927, his path through life was not an easy one, as was the case for many of his generation. He was called up as a soldier straight from school and only obtained his school leaving certificate after the war. This enabled him to embark upon the study of mathematics which he completed in 1953, having received his doctorate.

He joined the Central Cryptography Office in 1953 as a young cryptologist. After working in various management positions, including as the head of mathematical cryptology, Otto Leiberich took over the leadership of a larger data centre and then became the head of the Central Cryptography Office in 1972.

As young employees back then – almost 25 years ago – we are and were very grateful to Dr Leiberich for opening up new possibilities and perspectives in the Federal Office for Information Security, which was founded in 1991. We experienced him as sincere, open and very genuine, both as a senior colleague and as a person, and well into his senior years with him maintaining a great interest in issues relating to cryptology and IT security.

We share in his family's sadness and will always remember him as a sincere and tireless person. ■

Calendar 2015

What the Federal Office for Information Security dealt with this year

7 January 2015:
DDoS attack on bundeskanzlerin.de
A series of DDoS attacks brings down the websites of the Federal Chancellor and the Bundestag for several hours.

14 January 2015:
Berlin forum on cyber security
The forum event established by the Federal Academy for Security Policy (BAKS) and the Federal Office for Information Security (BSI) is held for the second time and focuses primarily on global aspects of cyber security.

20 – 22 January 2015:
OMNICARD
This year's OMNICARD addresses issues relating to electronic identification in areas such as electronic payment systems, e-government, cyber security, smart homes and e-health.

10 February 2015:
Safer Internet Day
"Let's create a safer Internet together" is the motto of this year's Safer Internet Day. The focal point of the event is how to achieve a better Internet for children and young people. More than 100 countries from all over the world take part in this annual day of action.

9 – 12 February 2015:
E-World
In the spotlight at the E-world trade fair are strategies, innovations and setting the course for the future of the energy market.

16 – 20 March 2015:
CeBIT
The main areas of focus for the Federal Office for Information Security at this year's CeBIT are the IT-Grundschutz and its ongoing development, Internet security, cloud computing, the Alliance for Cyber Security and secure solutions for mobile communications..

8 – 9 April 2015:
Cyber attack on TV5 Monde
French television network TV5 Monde is the victim of a cyber attack. Broadcasting is temporarily brought to a complete standstill. The broadcaster's websites and social media channels are also out of action for several hours.

13 – 17 April 2015:
Hannover Messe
The hot topic at the Hannover Messe trade fair is Industry 4.0. The Federal Office for Information Security has its own stand where it provides information on the challenges of cyber security and IT security in relation to industry. The live demonstrations show potential attack scenarios on industrial facilities and examine protection options.

16 – 17. April 2015:
Federal Office for Information Security/a-i3 symposium
The working group Identity Protection on the Internet looks at how to protect identity and identification data on the Internet. In cooperation with the Federal Office for Information Security, the symposium meets for the tenth time at the IT Security Building in Bochum and presents, among other concepts, the trusted cloud data protection profile for cloud services.

8 May 2015:
ITS.Connect job fair
The Federal Office for Information Security takes part in the careers fair for IT security at Ruhr University Bochum to promote itself as an attractive employer to students and graduates.

15 May 2015:
Cyber attack on the German Bundestag
The Federal Office for Information Security helps IT experts from the Bundestag parliamentary administration analyse the cyber attack incident.

19 – 21 May 2015:
14th German IT Security Congress
"Know the risks, accept the challenges, design the solutions" is the motto of the 14th German IT Security Congress. The issues examined include protection against risks in cyber space and the intensive cooperation required between the state, industry and academia.

7 – 8 June 2015:
G7 summit, Schloss Elmau
Increased cyber security is also a hot topic at the meeting of the seven heads of state and governments in Bavaria.

8 – 9 June 2015:
German Congress on Crime Prevention
The key focus of the congress in Frankfurt/Main is "Prevention pays off. The economics of crime prevention." In addition to organising the congress, the German Congress on Crime Prevention provides information and documentation on crime prevention.

11 – 12 June 2015:
Potsdam Conference for National Cyber Security
Organised by the Hasso Plattner Institute, the conference brings together representatives from the worlds of politics, administration, business and academia to discuss opportunities for action for cyber security.

14 – 19 June 2015:
27th Annual FIRST Conference
At the annual conference of the international association of computer incident response teams (FIRST) in Berlin, representatives from international CERTs share information on IT security issues and develop approaches for possible concepts to improve the future of IT security.

25 July 2015:
IT Security Act becomes effective
The Act to Improve the Security of Information Technology Systems (IT Security Act) addresses critical infrastructure operators in particular as well as the operators of websites, and leads to an improvement in IT security in Germany, benefiting industry and private users.

Calendar 2015

What the Federal Office for Information Security dealt with this year

22 – 23 August 2015:
FrOSCon conference
The computer science department of the Bonn-Rhein-Sieg University of Applied Sciences works in cooperation with FrOSCon e.V. and LUUSA (Linus/Unix user group) to give presentations and workshops on open source and free software. The Federal Office for Information Security has a stand at the conference.

29 – 30 August 2015:
Federal government open days
As every year, the German government invites the public to its open days in Berlin. The Federal Office for Information Security has stands at the Federal Ministry of the Interior and the Federal Press Office, where it provides information on IT and Internet security.

1 September 2015:
Digital Society Forum
The series of events examines key issues involved in the ongoing digitisation of society and presents these for debate. The forum is launched on 21 August with the expert panel discussion at the Federal Ministry of the Interior on “Big data – a challenge for data protection.” This is followed by a dialogue round on 1 September with Thomas de Maizière on "Protecting citizens and online retail from cyber crime."

23 September 2015:
UP KRITIS meeting
The public-private collaboration between critical infrastructure operators (KRITIS), their associations and relevant government bodies meets at the Federal Press Office to discuss “The protection of critical infrastructures – cooperation and regulation”.

October 2015:
European Cyber Security Month (ECSM)
The month of action is part of an EU-wide campaign to promote cyber security among citizens. The aim is to raise awareness of cyber security among Internet users in Europe and provide assistance. The Federal Office for Information Security works with various partners to coordinate activities for the ECSM in Germany.

6 – 8 October 2015:
it-sa
At the IT security exhibition in Nuremberg, security officers, developers and providers learn more about key issues relating to IT security including cloud computing, IT forensics, data security and hosting.

18 – 19 November 2015:
National IT Summit
The National IT Summit provides a platform for politics, business, academia and society to discuss the shaping of digital change. Key themes from the German government’s digital agenda are addressed and worked on as part of specific projects. The results are presented at the IT Summit in Berlin.

Legal Notice
Published by: Federal Office for Information Security (BSI), 53175 Bonn, Germany
Source of supply: Federal Office for Information Security (BSI),
Section B23 – Press and Public Relations, Godesberger Allee 185–189, 53175 Bonn, Germany
Telephone: +49 (0)228 99 958 20; email: oeffentlichkeitsarbeit@bsi.bund.de; Internet: www.bsi.bund.de
Project manager: Stephan Kohzer
Date: September 2015
Content and editing: Federal Office for Information Security (BSI)
Concept, editing and design: Fink & Fuchs Public Relations AG, Berliner Straße 164, 65205 Wiesbaden, Germany. Internet: www.ffpr.de
Image credits: Title: Steffen Kugler/Federal Government; p. 2: ra2studio/Shutterstock (top left), Rawpixel/Shutterstock (top right); Steffen Kugler/Federal Government (bottom left), FWStudio/Shutterstock (bottom right); p. 3: BSI; p. 4: ra2studio/Shutterstock; p. 5: ra2studio/Shutterstock; p. 6: BSI (left), ra2studio/Shutterstock (right); p. 7: Photonyx Images/Shutterstock (top), BSI (centre right); p. 8: Photonyx Images/Shutterstock (top); p. 9: Photonyx Images/Shutterstock; p. 12: Steffen Kugler/Federal Government; p. 13: BSI; p. 14: maraga/Shutterstock (top), BSI (bottom); p. 15: maraga/Shutterstock, BSI (bottom left), BSI (top right); p. 16: Alexandru Marian/Shutterstock; p. 17: BSI (top left), BSI (bottom left); p. 19: Alexandru Marian/Shutterstock; p. 21: urbans/Shutterstock; p. 22: Daniel Kunzfeld/BSI; p. 23: Daniel Kunzfeld/BSI (bottom left), Daniel Kunzfeld/BSI (top right); p. 24: Daniel Kunzfeld/BSI (top left), Daniel Kunzfeld/BSI (bottom left), Daniel Kunzfeld/BSI (top right), Daniel Kunzfeld/BSI (centre top right), Daniel Kunzfeld/BSI (centre bottom right), Daniel Kunzfeld/BSI (bottom right); p. 25: Daniel Kunzfeld/BSI
(top left), Daniel Kunzfeld/BSI (centre bottom left), Daniel Kunzfeld/BSI (bottom left), Daniel Kunzfeld/BSI (top right), Daniel Kunzfeld/BSI (centre top right), Daniel Kunzfeld/BSI (centre bottom right); p. 26: Rawpixel/Shutterstock (top), BSI (bottom); p. 27: Rawpixel/Shutterstock; p. 28: BSI (centre top), BSI (centre bottom), Rawpixel/Shutterstock (right); p. 29: BSI (centre bottom), hitmanphoto/iStock; p. 30: hitmanphoto/iStock; p. 31: hitmanphoto/iStock; p. 32: hitmanphoto/iStock (top), BMI (centre); p. 33: LoloStock/Shutterstock (top), BSI (bottom); p. 34: gui jun peng/Shutterstock; p. 35: gui jun peng/Shutterstock; p. 36: gui jun peng/Shutterstock (top), BSI (centre left), Piotr Adamowicz/Shutterstock; p. 37: gui jun peng/Shutterstock (top), Gencho Petkov/Shutterstock (bottom); p. 38: Den Rise/Shutterstock; p. 39: Den Rise/Shutterstock; p. 40: Daniel Kunzfeld/BSI; p. 41: Daniel Kunzfeld/BSI; p. 42: BSI; p. 44: Steffen Kugler/Federal Government (centre bottom), BSI (top right); p. 45: BSI (top left), Steffen Kugler/Federal Government (top right), K. Herschelmann/Hasso Plattner Institute (centre right); p. 46: BSI (centre), Rainer
Jensen/dpa (bottom right)
Printing: Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 63086 Frankfurt/Main, Germany. Internet: www.zarbock.de
Item number: BSI-Mag 15/702e
The Federal Office for Information Security magazine is published twice a year. It is part of the Federal Office for Information Security’s public relations work. It is provided free of charge and is not intended for sale.

www.bsi.bund.de