



Federal Office  
for Information Security

# Security in focus

BSI Magazine 2016/01



25 Years of the BSI

More security thanks to transparency



## Dear readers,

In this issue of the BSI Magazine, we are looking back at a quarter of a century of German IT security history, because this year the Federal Office for Information Security is celebrating its 25th anniversary. The threat of computer viruses was an issue for the BSI already in the 1990s, the “early years of IT security”. At that time, computer viruses and worms were still exotic; there were only one or two new viruses per month. The BSI’s answer to this first challenge was antivirus floppy disks, which today would be hardly conceivable.

The “I love you” virus, which caused an estimated 10 billion dollars damage in the early 2000s, raised public awareness of cyber security, which before had been considered a niche topic, for the first time. The “Millennium bug”, or the “Year 2000 problem”, concerned not only German computer owners, but also required considerable effort of the federal administration, and led to massive preparations for its potential failure. The case of the malware Stuxnet in 2010 shows that also major industrial infrastructure sectors are no longer safe from targeted IT attacks. Stuxnet was the first malware able to attack process control systems of industrial plants. In 2012, the programs Duqu and Flame further raised awareness of “cyber security” due to their high functionality and complexity.

Since the establishment of the BSI in January 1991, therefore, both the threat situation and the technical means to protect against cyber attacks have changed fundamentally. Also the legislation, on which the tasks, rights and obligations of the office are based, has been adapted to current developments time and again, and has given the BSI adequate resources for preventive security.

This is one of the reasons why the BSI is now well prepared to respond rapidly, for example in case of attacks on the federal administration. This is important, because dealing with a cyber espionage attack is not a daily business for the institutions concerned, and can involve several hundred man-days. This issue informs what happens when prevention fails, and how the BSI handles such incidents.

The foundations for the Internet of Things are being laid throughout Europe. The global networking of IT systems creates the possibility of incidents in information infrastructure of other countries indirectly affecting Germany. Therefore, we also look forward to a future market for cyber security: automated driving. The use of assistance systems that autonomously steer the vehicle, change lanes, and brake in an emergency will be allowed for the first time in 2016. New com-



Arne Schönbohm,  
President of the Federal Office  
for Information Security (BSI)

munication options open the vehicles to the outside world, and thus expose them to potential abuse. The BSI is already working on the development of an appropriate IT security concept to secure the communication between vehicles and traffic control units. We would like to present that concept in the current BSI Magazine.

I hope you’ll find our new issue an inspiring read with many interesting insights into known and new issues of cyber security.

Bonn, March 2016

Arne Schönbohm,  
President of the Federal Office  
for Information Security (BSI)





08

Interview with Guus Dekkers,  
CIO Airbus and Airbus Group



20

Cloud computing



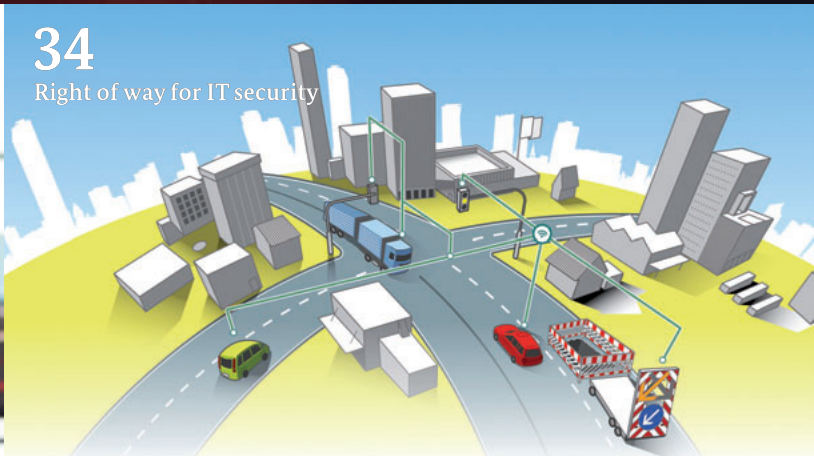
26

More security thanks to transparency:  
25 Years of the BSI



43

Invitation to the workshop



34

Right of way for IT security

---

## NEWS

---

- 6 In brief

## CYBER SECURITY

---

- 8 “There is no place for compromises  
in questions of security.”  
Interview with Guus Dekkers
- 12 When prevention has failed: Prerequisites for  
successful management of cyber espionage cases
- 16 2015 Cyber Security Survey:  
The number of successful  
cyber attacks is on the rise

## DIGITAL SOCIETY

---

- 18 “There is a lot to do!”  
Interview with Klaus Vitt, Secretary of State  
at the Federal Ministry of the Interior  
and Federal Government Commissioner  
for Information Technology
- 20 Cloud computing:  
The game changer for information security
- 23 Maximum counterfeit protection:  
Ten years of electronic ID documents

## 25 YEARS OF THE BSI

---

- 26 More security thanks to transparency:  
25 years of the BSI
- 33 25 years of the BSI Act:  
The development of responsibilities  
and powers

## IT SECURITY IN PRACTICE

---

- 34 Right of way for IT security:  
Intelligent transport systems
- 40 Secure communication in the digital age:  
With an application-oriented combination  
of measures in practice

## THE BSI AND ITS RESPONSIBILITIES

---

- 42 The new president of the BSI,  
Arne Schönbohm, takes office
- 43 Invitation to the workshop:  
New format of media dialogue
- 44 Innovative and yet still relevant to  
everyday life: The BSI as an employer

# In brief

## BSI President Hange retires

On 11 December 2015 in Bonn, the Minister of the Interior, Thomas de Maizière, bid farewell to the previous President of the BSI, Michael Hange, on the occasion of his retirement. Hange had been heading the Bonn agency since October of 2009. He left the office on 30 November 2015, having reached retirement age.



## IT situation report presented in Berlin in 2015

On 19 November 2015 in Berlin, the Minister of the Interior, Thomas de Maizière, and the former BSI President, Michael Hange, presented a report on the state of IT security in Germany. The report describes and analyses the current IT security situation, the causes of cyber attacks, and the attack means and methods used. Derived from this, the report focuses on solutions to improve IT security in Germany.



The report is available at [www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation\\_node.html](http://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html).

The screenshot shows the BSI website's new design. The header includes the BSI logo, language options (LEICHTE SPRACHE, GEBÄRDENSPRACHE, ENGLISH, KONTRAST, LÖSUNG), a search bar, and a navigation menu (Themen, Das BSI, Presse, Publikationen, Service). The main content area is titled 'Aktuell' and features a grid of news items and events. The news items include 'Safer Internet Day: BSI informiert über Risiken durch Ransomware', 'Verschlüsselung: BSI veröffentlicht Studie zu OpenSSL', and 'Regelungen im Rahmen des IT-Sicherheitsgesetzes'. The events section lists 'Common Criteria CC-ZERTIFIKAT BSI-DSZ-CC-0901-2015' and 'Präsentationsschwerpunkte und Vorträge des BSI auf der CeBIT'. A 'Termine' section on the right shows a calendar with dates 15, 16, and 02, corresponding to 'Schulung "Notfallmanagement ..."', 'E-world', and '12. Cyber-Sicherheits-Tag'.

## Relaunch: New design of BSI web pages

The BSI has redesigned its web pages comprehensively: the pages appear tidier, the design has been modernised, the user experience has been improved, and the pages adjusted to better suit the needs of mobile device users. The internet sites of the BSI can be found under [www.bsi.bund.de](http://www.bsi.bund.de), [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de), and [www.allianz-fuer-cybersicherheit.de](http://www.allianz-fuer-cybersicherheit.de).







### **Business protection: Telekom certified for counter-surveillance**

The German Telekom is the first institution to be certified by the BSI as IT security service provider in the field of “counter-surveillance in business”. The German Telekom has proven to meet certain minimum quality standards in the planning, execution, and evaluation of counter-surveillance tests. The company is also an expert in the application of a wide range of test methods. The independent BSI certification is intended to help companies find qualified service providers in the field of counter-surveillance.

### **IT Security Act: A draft of KRITIS directive is available**

The Federal Ministry of the Interior has submitted the draft bill of a directive for determining critical infrastructure (BSI KritisV) to federal states and organisations in February 2016; the directive supplements the IT Security Act. The Act sets out, inter alia, that operators of critical infrastructures are obliged to implement minimum standards, and must report IT security incidents to the BSI. The directive allows the operators of critical infrastructure to check whether they fall within the remit of the IT Security Act using measurable and comprehensible criteria.



### **CSCG: Young hackers wanted**

To safeguard the digital future of Germany, the Institute for Internet Security – if(is) and TeleTrust IT Security Association Germany will hold a “Cyber Security Challenge Germany – CSCG” ([www.cscg.de](http://www.cscg.de)). They are looking for the best young German hackers between 14 and 30 years of age, who will be solving online challenges from May 2016. Those who succeed in the final test in Berlin in September will take part in the European Cyber Security Challenge (ECSC).

### **Analysis: TrueCrypt is still suitable for encryption**

The German Federal Office for Information Security (BSI) commissioned the Fraunhofer Institute for Secure Information Technology (SIT) to carry out a security analysis of the encryption program TrueCrypt. The result: TrueCrypt is still suitable for encryption of data on data carriers. The complete TrueCrypt analysis is available at [www.bsi.bund.de/Studien](http://www.bsi.bund.de/Studien).



### **European Cyber Security Month**

In October 2016, the BSI will participate again in the European Cyber Security Month (ECSM, <https://cybersecuritymonth.eu>). The BSI will assume the role of the coordinating body. The action month is held annually across Europe under the auspices of the European IT security agency ENISA (European Union Agency for Network and Information Security). Its aim is to raise awareness of cyber security between citizens, companies and organisations. Last year, the BSI defined four key topics, which were successfully dealt with during ECSM.



# “There is no place for compromises in questions of security”

## Interview with Guus Dekkers, CIO Airbus and Airbus Group

*The Dutch Guus Dekkers has been CIO of Airbus Group since 2008, and has since received much praise, especially for the integration of various innovations in the corporate IT. Nevertheless, high-tech companies, to which Airbus Group undoubtedly belongs, are in the focus of cyber attackers. He explained in the interview that cyber defence is a key part of corporate activities.*

### **To what extent has the cyber risk situation changed for Airbus Group in recent years?**

The risk situation has changed in two respects. On the one hand, the focus of cyber threats has shifted away from the core company towards smaller affiliates or our supply chain. This development is understandable, because we have made substantial investments to secure our core processes in recent years. If the front door is much better protected, the cyber attackers will increasingly target the back door; we are aware of that.

The second development we have observed is that attacks are better tailored to the individual targets. For example, malware is designed specifically for a one-time special application scenario, and is used to gain access. The lack of predictive testing algorithms makes the identification of such intrusion attempts more difficult. In particular, smaller companies have difficulties to counter such unusual attack scenarios.

### **From your point of view, what types of cyber attacks should companies expect in the coming years?**

A few years ago, the key challenges for corporate IT managers were protecting intellectual property and inhibiting financial fraud. Meanwhile, however, the focus is on the corporate value chain. It is the responsibility of IT departments to block threats that may affect the corporate value creation process, because software is part of the majority of our products. Many of them are part of a networked environment. The intelligent networking of devices and machines, which is summarised under the term “Internet of Things”, brings special demands in terms of safeguarding and product liability itself. A failure caused by a cyber attack can significantly affect the reputation



### **Profile: Guus Dekkers**

Guus Dekkers has been CIO of the Airbus Group and CIO of the company's Airbus Division since 2008. As such, he is responsible for all IT systems and architectures employed by the Airbus Group worldwide. Before joining Airbus, Dekkers had worked for 18 years at renowned companies in the automotive sector, such as Volkswagen, Johnson Controls, Siemens, and Continental. During that time he held various IT positions and was finally promoted to CIO. Dekkers gained experience in various countries, including Germany, France and Mexico. The professional magazine *Computerwoche* chose Dekkers as “CIO of the Year” in 2013. The Dutchman has a degree in computer science from Radboud University Nijmegen, Netherlands, and an MBA (Master of Business Administration) from the Rotterdam School of Management. Dekkers and his family live in Toulouse, France.





“We have set up specialist teams with the aim to conceive and design our products as already ‘cyber-safe’ in the development stage.”





and growth of a company. One can easily imagine what an incident would mean for Airbus Group.

The result is that our tasks in the field of IT security have increased significantly, and not only in the field of classical information and communication technology. The expenses have tripled in recent years, so that we now invest tens of millions a year in our IT security. Our aim is also to ensure that our products are “cyber safe” in the design stage. We have created dedicated teams to this end.

***IT security is often associated with the necessity to change use patterns. How do Airbus Group's employees deal with this challenge?***

The unfortunate fact that many employees have had negative experiences with cyber attacks in their personal environment helps in this regard. It makes it easier for us to make our employees aware of certain behaviours. However, for many people the risk situation remains very abstract and difficult to assess in a particular case – along the lines of: “What you cannot see will not cause you harm.”

***About the Airbus Group***

The Airbus Group is a world leader in aerospace and related services. The turnover amounted to €60.7 billion in 2014, and the number of employees was 138,600. The Group includes Airbus, Airbus Defence and Space, and Airbus Helicopters.

*A glance at the control centre of Airbus A350 XWB: the cockpit combines high-tech, comfort, and maximum safety.*

We conduct broad and continuous education campaigns to address this, such as e-learning offerings, entertaining videos meant to increase awareness, as well as seminars with live hacking sessions, which are very well attended. Nevertheless, the interplay between the expected usage comfort, new functionalities, the available budget, and the necessary safety measures is very complex. Often, user comfort of the individual is placed above the important fundamentals of IT security, with expectations that correspond to the unlimited possibilities from the private environment. Unfortunately, there is a lack of understanding when certain actions must be rejected because of concerns about IT security.

***When it comes to the contribution of IT security to the corporate value creation, how do you measure the benefits of the necessary security expenditure in corporate IT?***

I like to compare the investment in corporate IT security to health insurance contributions. If you choose a better health insurance and pay the related costs in the long term, there is no guarantee that you will stay healthy. Nevertheless, you have definitely made the best possible arrangements. Conventional economic criteria can never tell if all investments were correct. The management, however, is aware of the industry-specific risks of carelessness in dealing with IT security, and does not want to compromise in that regard. For this reason, we have had a group-wide IT security programme for several years now, which reports directly to the management and is equipped with suitable financial means. However, this approach can be quite different in other industries.

***Are you able to demonstrate, through indicators, how much better your risk assessment is?***

Yes, certainly. Our cyber-monitoring centre monitors the current risk situation 24 hours/7 days a week. Thus, we have continuous analyses available. We discover every month an average of 180 so-called zero-day exploits, i.e. malware that cannot be easily detected using conventional methods. Furthermore, we inform about 40 website operators per month on average that their websites have been hijacked and misused for cyber attacks. The majority of those affected are very grateful for such information, yet they are also very surprised.

***If you could make a wish, what role would industry associations and public institutions play in IT security in the future?***

I'm more worried about German small and mid-size businesses than about larger enterprises. Corporations are quite capable of monitoring the threat landscape to properly assess it and to carry out the necessary actions. This is more difficult for German SMEs (small and medium enterprises). Keeping in mind that small and medium enterprises are the key innovators and the engine of the German economy, ways must be found to support them even more when it comes to IT security. I see this as one of the tasks of industry associations and public institutions.

Airbus Group has learned over the past few years how advantageous the cooperation on "situational awareness" in the interpretation of the threat landscape is for all parties. If cooperation is based on trust, the regular exchange helps to establish "best practices" and to jointly deal with current threats. Scarce financial resources can thus be used as efficiently as possible.

***What do you think will the future bring?***

We should make it clear that the subject of cyber crime is not gone, and has not been sustainably diminished. The currently visible IT security issues are only the beginning. The quickly evolving networking in the industry, and the increasing growth and dependence on IT solutions will ensure that IT security will be one of the key issues on our agenda. I think, therefore, it is mandatory for any management to deal with it as a matter of urgency. ●

# When prevention has failed

## Prerequisites for successful management of cyber espionage cases

*Currently, IT security firms outdo one another releasing new cyber espionage attack campaigns. They often focus on aspects of the malware used and summarise the effects on the institutions in one sentence. They forget to mention that these publications relate in most cases to incidents with analytic expenses of several hundreds of man-days. For those affected, successful management of an incident is noteworthy. This article presents a framework for sustainable management of such an event.*

### Contact

Experience shows that serious network infiltrations are reported in most cases by third parties to the institution concerned. The reason is that many institutions only have protection mechanisms against initial attack vectors. Once these are undermined, the institutions concerned do not have means to detect the activity of offenders to its own network. Therefore, most of the massive network infiltrations are only revealed when external bodies carry out major attack campaigns, and in this context investigate control servers of the perpetrators. The malicious programs that are installed in the affected networks connect to these servers. By evaluating these connections, analysts or investigators can infer and inform the institutions concerned.

Analysts in Germany often do not contact the institutions concerned directly; instead, they turn to the BSI as a central point of contact. The BSI is obliged to review the incidents in consultation with other security authorities, and to inform those concerned.

The information about connections to control servers which the BSI receives are essentially timestamps, IP

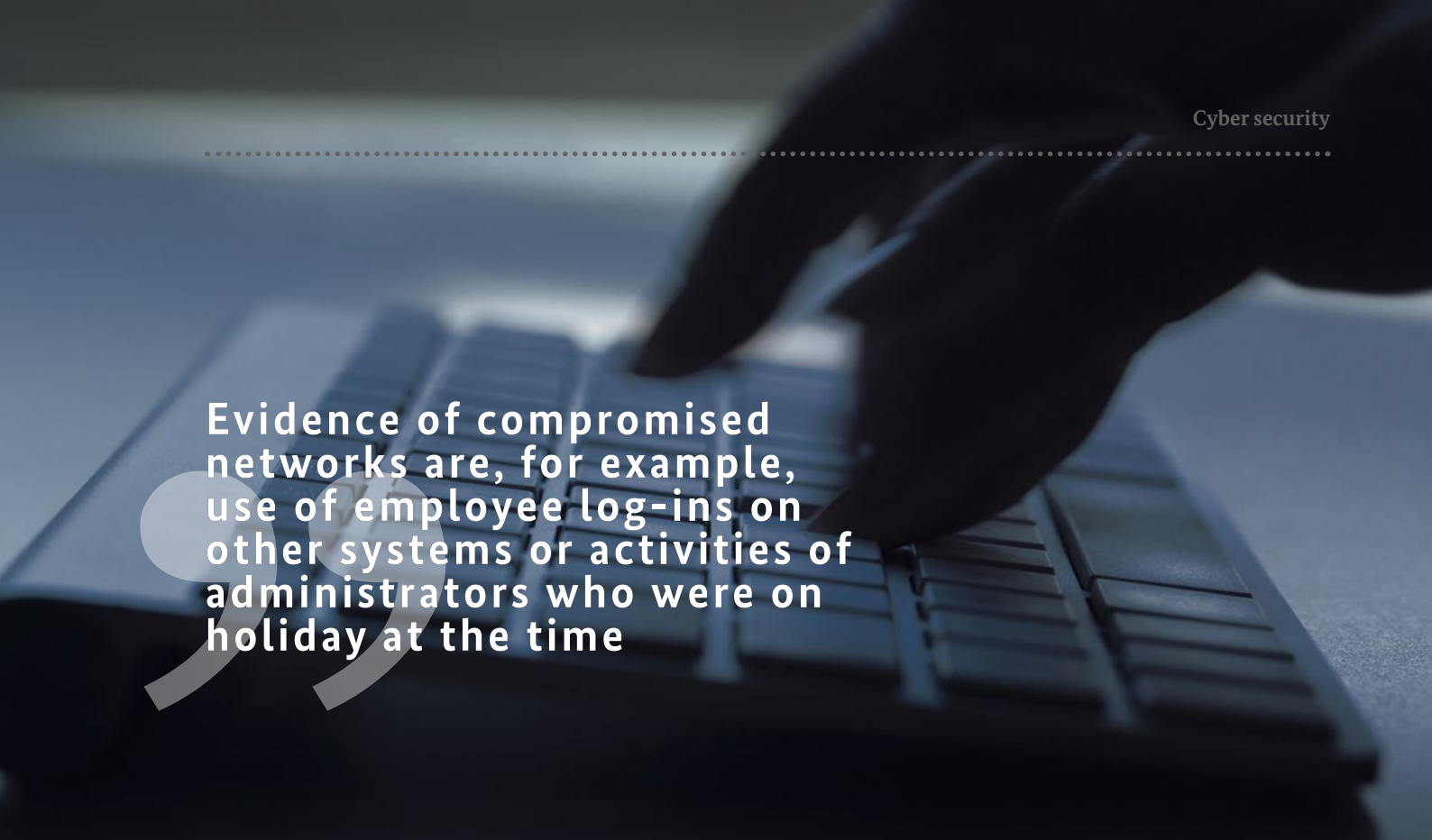
addresses of the computers concerned, and the address of the control server; often it is also the name of the malicious software that has been used. Unlike ordinary malware, such as banking trojans, cyber espionage programs are designed to allow the perpetrators to enter into the internal network and to support the so-called lateral movement. In other words, the perpetrators move from one internal system to another until they have reached the data that they are interested in. Based on the initial information received by the BSI, it is in most cases not possible to estimate how many computers in the network of the institution concerned are infected, and how deep the penetration into internal areas is. It is also a challenge for the employees of the affected IT operations to investigate whether and how many computers are affected.

Although this is very complex, it is in the interest of the institution concerned to undertake such an investigation on its own. The BSI must convey that in case of attacks by professional cyber espionage groups, it is not enough to clean up the computer from which the connections to the control server have been initiated. Instead, it is necessary to examine to what extent the perpetrators

have compromised the network. To this end, central log data must be evaluated in detail. The evidence of the activities of the perpetrators is often indirect: examples include activities by administrators who were on holiday at the time the activity was carried out, the copying of stolen data, overflowed disks, or log-ins from users on external systems. Often the required log data are not stored for long enough, nor are they available in sufficient detail; also, both staff council and data protection officers often see no sufficient reason to release the log data. In addition, the institution concerned often does not have the necessary know-how to examine log data with regard to such abnormalities. Since the BSI has limited resources, it sometimes recommends to commission external service providers.

Another point that needs to be addressed immediately after contact has been established concerns the internal communication. Usually such incidents in the institution concerned are first kept secret, and processed only by a few insiders. It can never be completely avoided that third parties become suspicious. When external service providers show up in the IT department, question the IT staff, and seize





## Evidence of compromised networks are, for example, use of employee log-ins on other systems or activities of administrators who were on holiday at the time

the computers, the circle of persons involved widens. A cover story may sometimes be created.

External consultants can influence how the institution concerned deals with the incident only to a limited extent.

Corporate culture, such as transparency in internal communications, or the importance that the company attributes to its own IT operations, are decisive in this regard.

### ***The analysis***

The analysis is typically performed by external service providers or BSI analysts. The first challenge is always to be able to work at the institution concerned in terms of technical analysis, since the analysts cannot work in the potentially compromised network; that is, they need their own infrastructure. This includes analysis workstations, internet access, servers for storing analysis results, a lot of space for copies of the hard drives to be examined, and fast servers to analyse gigabytes of log data. As banal as it

sounds, the preparatory actions take a few days, and also need the consent of the institution concerned. Demands for night operations and hourly results are unrealistic when it comes to network infiltrations.

IT employees and relevant supervisors in the institution concerned often fear being made a scapegoat. This sometimes leads to attempts to cover up alleged own mistakes by installing missed security updates, or carrying out additional security measures that overwrite the traces of the perpetrator. Moreover, the fear of recriminations undermines an open and constructive work environment in which administrators can use their knowledge of the network. Therefore, the BSI always makes clear that the purpose of the investigation is not to find the culprits, but to rectify the network infiltration and to guard against future attacks.

Immediate clean-up of infected systems alone is not effective because the perpetrators may have already infiltrated deep into the internal network, and

may have compromised other systems or access data (not yet identified). Therefore, the objective of the analysis is to determine the extent of the incident, and to understand the methods of the perpetrators. This process is iterative. The known technical details are processed into signatures to search the network for additional traces of the perpetrator. If other systems or artefacts are found, they are investigated to generate new indicators. These can then be used to re-scan the network. If no new insights are gained through such a loop, this indicates that the analysis can be completed successfully.

Typically, many different types of data are evaluated. Hard drives are analysed to find malicious programs and to investigate what the offenders have done to the systems. Firewall and proxy log data are evaluated for feedback channels and data outflow. Log data of directory service give evidence of atypical log-ins that indicate compromised credentials. Network recordings are examined in order to decipher encrypted traffic of the offenders. Detection

tools specially adapted to the incident are rolled out on all systems in the network and their log data is analysed. Last but not least, malicious programs are analysed to elaborate indicators for detection.

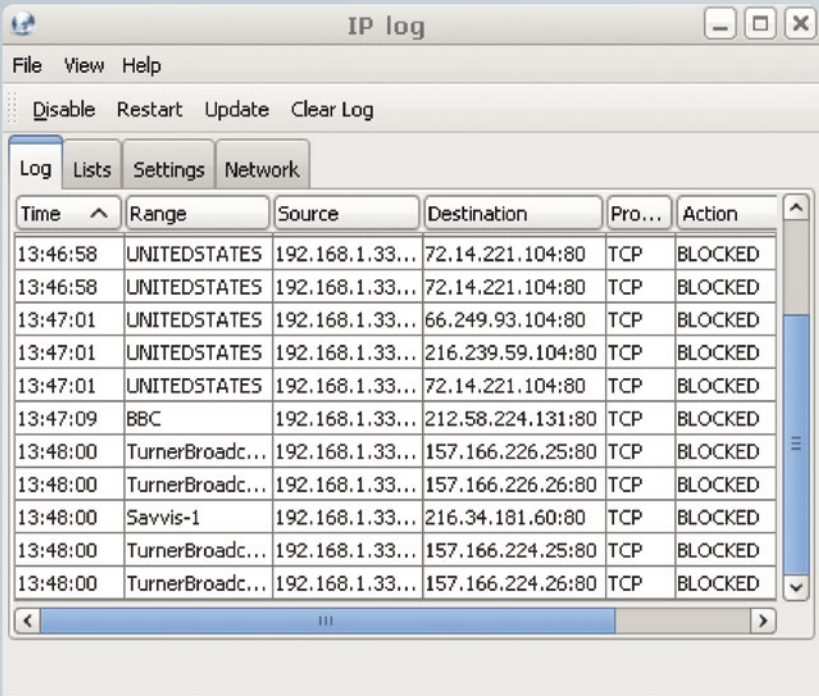
It is obvious that only a team of experts can have this analytical capability. The BSI does not provide a ready-made team that can react on demand; instead, it calls in experts from several areas where necessary. Individual analytic tasks can be performed by service providers in the case of limited resources.

External influences

The analysis is not isolated from the rest of the world. It generates legitimate questions from users whose computers need to be copied and inspected. It drives the concern whether it is safe to work on confidential documents, or whether it must be assumed that offenders had or have access to emails and files. Such analyses always have a technical and a public awareness component that need to be weighed against each other. Things get more difficult when employees start to speculate and make inaccurate statements about the condition of the network because of the scarcity of information provided to them.

The result

The so-called “patient zero” refers to the first infected system, which cannot be identified in all cases. This is because the attack has often taken



The screenshot shows a window titled "IP log" with a menu bar (File, View, Help) and buttons (Disable, Restart, Update, Clear Log). Below are tabs for Log, Lists, Settings, and Network. The "Log" tab is active, displaying a table of blocked connections.

Time	Range	Source	Destination	Pro...	Action
13:46:58	UNITEDSTATES	192.168.1.33...	72.14.221.104:80	TCP	BLOCKED
13:46:58	UNITEDSTATES	192.168.1.33...	72.14.221.104:80	TCP	BLOCKED
13:47:01	UNITEDSTATES	192.168.1.33...	66.249.93.104:80	TCP	BLOCKED
13:47:01	UNITEDSTATES	192.168.1.33...	216.239.59.104:80	TCP	BLOCKED
13:47:01	UNITEDSTATES	192.168.1.33...	72.14.221.104:80	TCP	BLOCKED
13:47:09	BBC	192.168.1.33...	212.58.224.131:80	TCP	BLOCKED
13:48:00	TurnerBroadc...	192.168.1.33...	157.166.226.25:80	TCP	BLOCKED
13:48:00	TurnerBroadc...	192.168.1.33...	157.166.226.26:80	TCP	BLOCKED
13:48:00	Savvis-1	192.168.1.33...	216.34.181.60:80	TCP	BLOCKED
13:48:00	TurnerBroadc...	192.168.1.33...	157.166.224.25:80	TCP	BLOCKED
13:48:00	TurnerBroadc...	192.168.1.33...	157.166.224.26:80	TCP	BLOCKED

The evaluations of firewall and proxy log data give insights into the activities of the attacker.

place long before the examination was started. Therefore not all required log data is available.

It is known, however, that professional perpetrators tend to use all types of attacks that exist in IT security. The most common are prepared emails that are tailored to the particular recipient, and contain a link to malicious code, or an attachment with malware. The so-called “watering hole attacks” are also widespread; here, sites that are relevant to the target audience are attacked and infected with malicious code. When the targeted persons visit the website, a back door is installed on their computers using the malicious code. The classic hacking, where web servers or other systems that can be

accessed via the internet from the outside are attacked, also still exists. Common to all these types of attacks is that the perpetrators do not stop with one initially compromised computer, but use it as an entry point to reach into the internal network. They download more malicious programs and tools, and look for stored log-in information in the memory.

The aim of the perpetrators is always to secure long-term access to the network. Access data with high system privileges are exceptionally valuable. With this access data, the perpetrators can freely propagate in the network and access sensitive systems. In many cases, one of their first targets is the domain controller that manages all

access data and authorisations in a network. If the perpetrators compromise it, the network is compromised fundamentally and cannot be cleaned up by exchanging individual computers. When perpetrators assume control of these central systems, they gain access to all access data, including VPN access data.

### **The clean-up**

One of the most contentious issues in each incident is whether you should instantly clean the infected systems and close the detected feedback channels immediately. As intuitive as this approach may sound, it is often counterproductive. These measures alert the perpetrators that they have been discovered, and that their activities are being examined. This makes them erase leads and change their methods. In the early stages of the investigation, the analysts do not yet know which malicious programs, tools, and access data the perpetrators use, and on which systems they have installed back doors; thus, the entire network cannot be cleaned up yet. The perpetrators will still have access, even if some computers are cleaned. Moreover, in most cases the perpetrators have already been active in the network for months, and may have already stolen much of the data which was of interest to them.

For these reasons, the BSI recommends investing the necessary time to fully investigate the incident at the beginning. This may take several weeks or months. Only when a coherent picture of the incident is present, can a plan to clean the network thoroughly and

protect it against future attacks be developed. For example, if the Active Directory has been compromised, there is no other way than to reset passwords in the entire organisation and rebuild the Active Directory.

To block future attacks of this kind, it is recommended to use a concept called ESAE - "Enhanced Secure Administrator Environment", which secures the Active Directory and administrator workstations, and isolates them from the rest of the network. It is assumed that a single infected PC will thus not be able to compromise the entire Windows domain. To prevent propagation in the network, connections between desktop PCs are blocked via personal firewalls and group policies in the domain controller.

To discover attacks faster in the future, it is advisable to implement a security monitoring concept that provides for continuous analysis of log and sensor data. In addition, users should be sensitised to be able to detect attacks via social engineering.

### **Conclusion**

The aspects that positively influence incident handling are, on the one hand, that the institution concerned treats the incident seriously, and does not marginalise it as part of its daily IT operations. Furthermore, instead of searching for culprits, constructive work should be done to block future attacks. It is crucial that the investigation is given enough time, and nobody

insists to perform a clean-up based on inadequate information when the full extent of the infiltration may not yet be visible. A clean-up of malicious code or a clean installation do not resolve a security incident. The defects identified by the analysing team must be rectified, and the proposed safety measures implemented to block future attacks, or at least make them less common. ●



*Timo Steffens,  
Section Situation Centre and CERT-Bund*

# The number of successful cyber attacks is on the rise

This is evidenced by the results of the 2015 Cyber Security Survey. The BSI carried out the cyber security survey for the second time, with the support of the Federation of German Industries (BDI), the German Association for Information Technology, Telecommunications and New Media (Bitkom), the Association of German Chambers of Industry and Commerce (DIHK), German Society for Computer Science (GI), the Association of IT Users (VOICE), the Association of Machinery and Plant Engineering Companies (VDMA), and the Central Association of the Electrical Engineering and Electronic Industries (ZVEI). The continuation of figures from the previous year shows that the cyber security situation remains tense for companies and authorities.

The survey was carried out as an online survey with 18 closed questions in the period from June to September 2015. Data from 424 corporate records were evaluated in total.

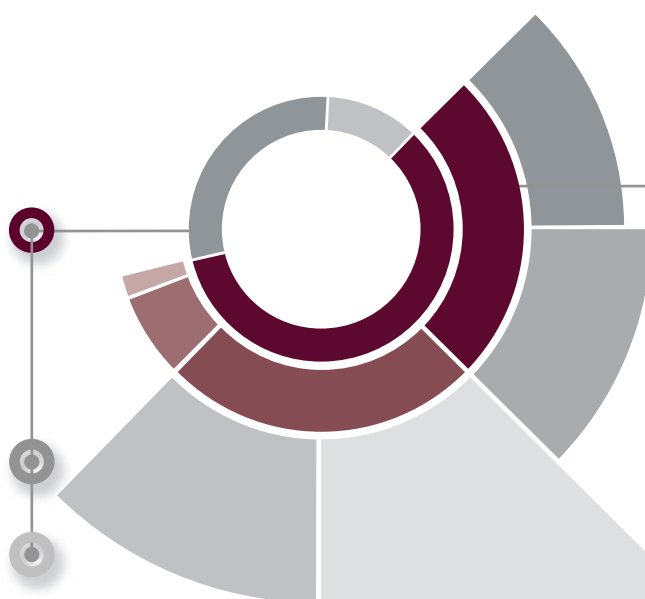
1

## Target of attacks

**58.5 %** of the institutions and companies surveyed have **found** that they were **targeted by cyber attacks**. This included both successful and blocked attacks.

**30.3 %** of the institutions surveyed did not experience any attacks.

**11.3 %** did not respond.



## Of the detected attacks...

**42.7 % could not be blocked.** The attackers were successful in these cases.

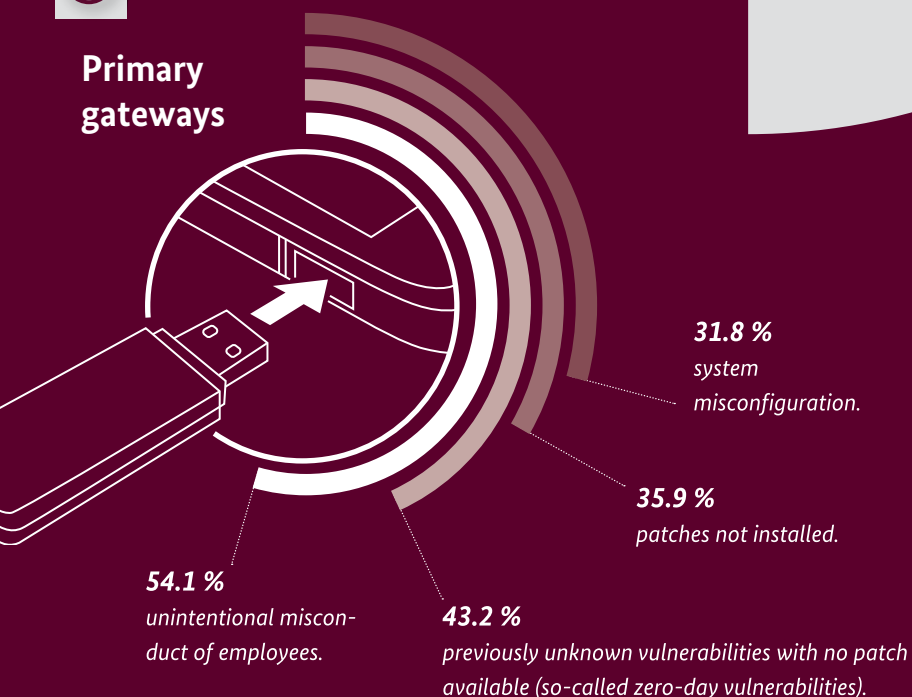
**42.3 %** were able to block the detected attacks.

**11.3 %** of cases reported an impact; however, it could not be unequivocally attributed to cyber attacks.

**3.6 %** did not respond.

3

## Primary gateways



2

## Type of detected attacks

**72.2 %** were random and **non-targeted infections with malware** through drive-by download via website banners or spam emails.

**30.6 %** were **DDoS attacks** on institutional websites.

**21 %** were **targeted infections** with malware through social engineering via email or USB stick.

**19.8 %** were attacks aimed at **taking IT systems over** to misuse them for attacks on other systems.



4

## Economic damage caused by attacks is difficult to quantify

19.1 % production and operational downtime.

15.1 % significant cost of investigation and system recovery.

8.5 % digital identity theft.

8.3 % reputational damage.

5.7 % theft of economically important data.

5

STOP

## Suspended operation

46.2% of the institutions surveyed had to suspend their operations temporarily following cyber attacks.

7

## The most threatening cyber attacks in the coming years

63% of the surveyed institutions expect **primarily targeted infections with malware** via drive-by downloads or spam emails,

59.2% expect **data theft** caused by systems penetrations,

47.4% **APT Penetration of systems** for the purpose of a long-term infiltration, and

46.7% **random infections with malware**.

6

## The pressure is increasing

70.2% of institutions noted increase of risks due to cyber attacks.

20.8 %

79.2 %

Deployment of safer browsers or safer browsing environments.

31.4 %

Yes

No

68.6 %

Structured Information Security Management (ISMS).

51.7 %

48.3 %

Regular campaigns to increase awareness of all employees.

52.8 %

47.2 %

Encrypting data carriers.

64.4 %

35.6 %

Structured or centralised patch management.

84.4 %

8

15.6 %

Decentralised defence against malicious programs using AV software on client/server systems.

85.6 %

The need to catch up on protection against cyber attacks: actions taken

14.4 %

Centralised defence against malicious programs via security gateway or mail server.

95.5 %

4.5 %

Securing network interfaces (security gateways, firewalls, IDS/IPS, etc.).

9

## Planning

59% of surveyed institutions plan to further improve their IT security in the medium term.

15.3% need improvement in key areas in the short term.



The complete results of the 2015 Cyber Security Survey are available at the following address:  
[www.cybersicherheitsumfrage.de](http://www.cybersicherheitsumfrage.de)

## “There is a lot to do!”

### Interview with Klaus Vitt, Secretary of State at the Federal Ministry of the Interior and Federal Government Commissioner for Information Technology

**Secretary of State, the Department of Information Technology, Digital Society and Cyber Security is part of your area of responsibility. That is a broad field. Where do you intend to define the specific priorities?**

I have defined four priority areas that I want to take forward as Federal Government Commissioner for Information Technology: the digitisation of the asylum procedure, the consolidation of federal administration IT, the consolidation of Federal Government IT networks, and IT and cyber security.

**What role will the last of these play?**

The security of information technology is the basis of any form of digitisation. IT and cyber security issues therefore play a central role in my area of responsibility. I regard the IT Security Act, which came into force at the end of July 2015, as an important first step towards ensuring Germany's IT systems and digital infrastructures are among the most secure in the world in the future.

**How would you describe the role of the Federal Office for Information Security (BSI) in this context?**

For many years, the BSI has been the German Government's competence centre for IT and cyber security matters; its professional expertise is recognised far beyond the field of public administration. It has a clear legal mandate, which we recently expanded significantly once again with the IT Security Act. The BSI has become the central player for operators of critical infrastructures on matters relating to IT security. These include minimum standards for IT security and

reporting obligations for significant IT security incidents. The BSI also takes an active role when it comes to security incidents: when any significant incidents are reported, the BSI must inform other operators as quickly as possible.

**Compared to Germany, other European countries do not have such a clear separation between the IT security authority and the intelligence service. Is this special path still the right one despite the threat level?**

The establishment of the Federal Office for Information Security in 1991 was a very wise and forward-looking decision. By separating the code breakers from the code makers, the Federal Office was able to build up a great deal of trust over the years among the public and particularly within the business community. This is essential for a successful partnership between the government and the private sector.

**It may well prove impossible to achieve complete IT security. Is there potential for optimisation nevertheless?**

Cyber security originates in a secure environment. Cyberspace is only as safe as the systems and infrastructures associated with it. Neither the government nor the business sector alone is able to achieve IT security in our country – everyone needs to make a contribution. Cooperation between government and industry will be crucial in order to guarantee IT security in the future.

**You have many years of experience in the private sector, having worked for software and computer manufacturers and also in telecommunications. Is the German economy generally aware of and sufficiently equipped to deal with IT security challenges?**

In areas where value creation structures are fundamentally changing, IT security is frequently not a top priority. However, my feeling is that, increasingly, it will be recognised as essential infrastructure. After all, there is no reliable production, no e-commerce without IT security. However, things will get complicated when it comes to implementation: where exactly is my threat level and how can I protect myself in an econo-

**The IT Security Act is an important first step towards ensuring Germany's IT systems and digital infrastructures are among the most secure in the world in the future.**



#### **Profile: Klaus Vitt**

Klaus Vitt (born 1952) studied communications engineering at the Federal Post Office University of Applied Science and mathematics at the University of Dortmund. After beginning his career with various IT companies and Bertelsmann AG, he spent ten years working in senior roles in the IT field at Deutsche Telekom AG. He worked at the Federal Employment Agency from 2006 to 2015, first as Director of Central IT and then as Chief Representative for IT and Process Management. Since October 2015, Klaus Vitt has been Secretary of State at the Federal Ministry of the Interior and Federal Government Commissioner for Information Technology.

mically feasible way? Do I need support, and who actually provides secure products and services that can be trusted?

#### **Where and how can things be improved?**

Going forward, we will only be able to guarantee the availability, confidentiality and integrity of data and information if the government and businesses work together even more closely than they have up to now.

We might also need to develop new ways of working together where necessary. With the Deutsche Cyber-Sicherheitsorganisation (German Cyber Security Organisation), we have embarked on a new path with the private sector.

#### **You mentioned the IT Security Act – the relevant regulations are currently being drafted in two phases. What has been your experience as regards the willingness to cooperate?**

We are consciously taking a cooperative approach with the IT Security Act. This involves a relationship built on trust between government and businesses. We are already experiencing this with the preparation of the regulation in UP KRITIS. In a few weeks' time, we will have incorporated four of the seven sectors covered by the Act – energy, water, food and ICT – in the regulation. The remaining sectors of transport and traffic, health, and finance and insurance will follow by the end of 2016. It has been possible to make such rapid progress largely as a result of the cooperative and committed working relationships with the economic sectors addressed in UP KRITIS.

#### **At the beginning of the interview, you also mentioned protecting the government's network infrastructure. Will this also involve working together with German businesses?**

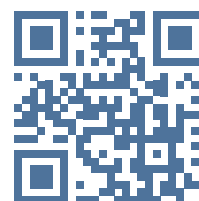
In order to continue protecting government and federal administration communications successfully in the future, we are pursuing a comprehensive consolidation programme called "Netze des Bundes" (Networks of Central Government). Trustworthiness plays a major role in the selection of efficient service providers for the project. It is crucial that the partner is willing and actually able to handle private information confidentially. It is also important that the data streams between the federal authorities remain in Germany at all times.

In this regard, we have had positive experiences in the past with German businesses and will therefore continue to work together with national partners in the future.

#### **You are an expert in this field and studied communications engineering, mathematics and IT. Was it possible to foresee the huge increase in the importance of IT security back then?**

Certainly not to this extent! The increasing digital vulnerability in all areas of our lives and business activities will become one of the main challenges for our society in the coming years. For all of us, that means there is a lot to do! ●

The Federal Government Commissioner  
for Information Technology:  
[www.cio.bund.de](http://www.cio.bund.de)





*Cloud computing has changed information processing sustainably. Individual physical data storage has been made largely unnecessary, and the technical development and usage patterns of mobile devices have been boosted, which has also changed the business world sustainably. In terms of IT security, cloud computing is a true “game changer” and it causes large revisions to information security.*

# Cloud computing

## The game changer for information security

*Cloud computing may have started as a hype five years ago; today, companies still have many questions about the security before they can actually start productive work in the cloud. But all signs indicate that a technology that will remain has developed from the hype. “The cloud is here to stay” – because it offers companies, whether as users or providers, future advantages if they make arrangements for their security now. Only those who know the consequences for IT security arising out of cloud computing are capable of acting.*

Fuelled by efficiency gains brought on by virtualisation, cloud users help their IT save on costs. Thanks to the broadband connections now widely available, IT resources, platforms and applications can be offered and used by numerous companies. For many IT managers the question “Buy or rent?” is new. Nowadays, if someone needs to create a report only once a year, they don’t need to buy software for several thousand euros, since the required service can be rented for less than fifty euros per month. The cloud manufacturers also

have advantages. Sales fluctuations for new versions of applications and programs are lower, because a relatively constant user base generates monthly revenues that can be better planned for. Sceptics see a potential for staff reductions in cloud computing, if IT operations are outsourced to cloud providers. But it is dangerous for businesses to believe that they can also simply outsource responsibility for their IT security.

What is certain is that the approach to IT security is changing dramatically for

many organisations such as security agencies and companies. This requires new processes and skills.

### **Game changer 1: Impact on the operation of security institutions**

Cloud computing is not only a new technology, such as a tablet compared to a laptop, it also causes significant changes to information security, which makes it a true “game changer”. This also has an impact on the activities of security agencies such as the BSI. So far, security evaluations are carried out



more or less as follows: New components or software are purchased and examined in the laboratory. Provided there is source code, it will be analysed. Questions such as, “Does the router pass data packets as it should?”, and, “Is the platform vulnerable while surfing the internet and, if so, why?” play a role for the evaluation of the employed product. However, it works only when components can be brought into a laboratory. Applications that are offered as a service on the internet cannot be investigated in this way. Besides, cloud providers are - when they're not in a certification process - usually not very eager to grant testing options. Outside of certification process, therefore, it is impossible to review the security of IT services with the proven methods.

#### ***Game changer 2: Change of corporate strategy***

The main positive economic aspect of cloud computing results from its mass usage, since high user numbers allow economies of scale, which will increase

the competitiveness and profits of the seller. The user will have little or no choice for or against the cloud in the future. Many large providers, such as Microsoft and Adobe, offer their products and services already mainly as a subscription model via the cloud. Microsoft explicitly pursues the strategy to develop only applications for its Microsoft Azure Cloud in the future. For the users, this means that whoever uses Windows or Microsoft Office, will procure their IT tools from the Azure cloud in the future. Whoever has security concerns, must thoroughly consider whether these are so severe that a full migration, for example to Linux and LibreOffice, would be acceptable.

#### ***Game changer 3: Impact on certification***

With the certification of information security management systems (e.g. ISO 27001) there is an implicit assumption that the auditor only gets to see the live system. Changes in the short term are too costly. In contrast, where cloud services are used, this thesis is no longer true, because a virtualised data centre can be moved quickly, and can be just as quickly completely

reconfigured. A complex zone system with many packet filters and so-called demilitarized zones (DMZ) has safety advantages, but it costs resources that could be made available to other customers. If the cloud provider employs the elasticity and flexibility to reconfigure the cloud infrastructure in the short term, it can use resources of security services for new customers. Current certification procedures cannot rule this out. In virtual infrastructures, technicians are not needed to redraw cables or restart servers. An administrator can perform all this by pressing a button. This raises the question of how valid and meaningful certificates will be in the future.

#### ***Fatalism is not an option: Secure cloud computing strategy***

As it turns out, cloud computing is a game changer which requires a new definition of IT security in many areas. It would be wrong to respond to these changes with fatalism, and to bury one's head in the sand. Secure cloud computing requires a great deal of trust, and trust can only be created through transparency. This can be defined in three areas:

#### ***BSI information on secure cloud computing***

The BSI website for secure cloud computing under [www.bsi.bund.de/cloud](http://www.bsi.bund.de/cloud) offers comprehensive materials for target groups, for CEOs and CIOs, as well as employees at the operational level. Furthermore, it offers extensive tips for risk analysis from a customer perspective.



Fatalism is not an option: Secure cloud computing strategy

1

Risk transparency

2

Open standards

3

Transparent breakdown of responsibilities of both users and providers

### **Transparency regarding risks (and opportunities) of cloud computing**

The BSI contributes to the transparency of risks in cloud computing by systematically recording and evaluating existing risks. The aim is to enable all users, from politics, business and society, to make well-informed decisions whether to use or not to use cloud services. It is necessary in this respect to distinguish between safe cloud computing and secure cloud. The ideal of a secure cloud is unattainable, because there is no absolute safety. It is crucial to make processes as safe as possible by analysing them in detail. Safe clouds are not the focus, secure cloud computing is. To this end, security requirements must be created and implemented in the course of cloud computing. This is an iterative and dynamic process. Whether a cloud service provider meets the requirements of the customer is a question of risk management, which must be carried out individually on the customer side. Two different customers of the same provider are highly likely to have two different opinions in this regard. Risk transparency means that you can make informed decisions. Risk transparency is therefore just as necessary as chance transparency.

### **Open standards create confidence for cloud computing**

Use of open security standards and disclosure of information regarding how the IT systems security is reviewed are among the basic requirements of the BSI. They also apply to the cloud. Risk management to assess the safety level of the business processes in the cloud must be considered to decide whether cloud computing is an option or not. The BSI therefore continuously works in cooperation with European partners such as the ANSSI in France to create open standards for secure cloud computing. The cloud computing catalogue of requirements can be audited with SOC 2 reports by auditors as part of ISAE 3000. It will not only determine if a request at any given time existed, but whether the associated measures have been implemented over a certain period.

### **Responsibility for security cannot be migrated to the cloud**

Responsibility cannot be outsourced, and state guarantees for security of cloud services, in the form of licensing, are not envisaged in the near future. Therefore, a clear division of responsibilities between users and providers is needed before cloud services are used. The user should contractually agree on all aspects of IT security that are relevant to them, both preventive as well as reactive measures. For this purpose answers to certain questions are needed: What happens during a

security incident? How is the chain of information regulated in case of failure? Is it possible to influence how the provider deals with the incidents? What are the consequences of possible violations of the agreements? The respective responsibilities must be clearly determined in advance, otherwise unorganised responsibility will turn into organised irresponsibility. ●



Dr Patrick Grete,  
Section Minimum Standards and  
Product Security

### **Security thrives on a dialogue: ask the BSI**

Risk assessments, safety measures, and safety standards can only be further developed in dialogue with cloud providers and users. You are welcome to send questions, comments and specific recommendations to [cloudsecurity@bsi.bund.de](mailto:cloudsecurity@bsi.bund.de). For questions regarding certification, send a message to [zertifizierung@bsi.bund.de](mailto:zertifizierung@bsi.bund.de).



# Maximum counterfeit protection

## Ten years of electronic ID documents

*For over a decade, electronic components have increased protection against forgery of official identity documents, sped up checks at airports and made the digital proof of identity on the internet possible. After the passport received an integrated electronic chip in 2005, the personal identity card and the electronic residence permit followed; today, all identity documents are now based on the same technical concept. The most recent addition is a new document: the proof of arrival for asylum seekers.*

### Passport

The passport with chip was introduced in Germany in two stages. Those issued after 1 November 2005 had a biometric photograph stored on their chips; two fingerprints were added to the chips on passports issued after 1 November 2007. Today, ten years after their introduction, all valid, centrally produced German passports contain such a chip. The ePass delivers an increase in efficiency at a high level of security by enabling the institution of automated processes at border control points. Any traveller with a European passport or

electronic identity card can now use the EasyPASS border control system at the busiest German airports. EasyPASS is able to verify the authenticity of a travel document in mere seconds as it performs a biometric comparison of the traveller's face with the photograph stored in the passport. The use of similar systems is increasing worldwide.

But electronic data enhance the quality of the conventional passport control process as well, as the authenticity of passports can be verified cryptographically and the chip provides the border

official with a higher-quality facial image.

### Identity cards

As a logical extension of the strategy for secure electronic identity verification, a new generation of identity card was introduced on 1 November 2010, followed less than a year later by the electronic residence permit (eAT) on 1 September 2011. In addition to their biometric function, the new documents also offer the means for secure identification over the internet (electronic

proof of identity), as required, for example, for eGovernment applications that allow citizens to easily complete administrative processes online, for which the identity card can be used to create an electronic signature (a qualified signature).

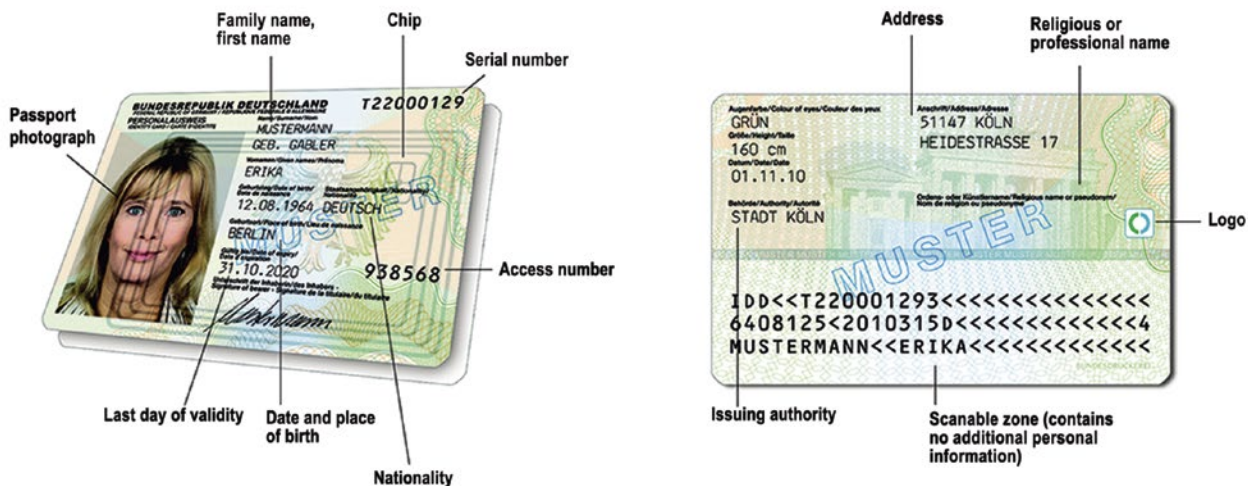
Five years after their introduction, some 40 million identity cards and new-generation residence permits have been issued, with the result that a majority of citizens are now equipped with this document, making it worthwhile for service providers to integrate this secure means of identification into their online processes and provide new services.

In pursuit of their eID strategy, the federal government and the federal states have also been setting up service accounts which citizens can log into with their electronic identity cards and which cover a vast number of administrative services delivered via the web. Other legislative initiatives have been started or are already completed. Under the eGovernment Act (E-GovG), German federal authorities are obliged “to provide identity cards and electronic residence permits with an electronic identity verification capability” for administrative proceedings “in which a provision of law requires them to establish a person’s identity”.

Client applications are continually being

**Technical family concept: one technology for all documents**

Several sets of specifications and protection profiles created by the BSI provide the technical backbone for all electronic ID documents – a modular, technical family concept. This means that the ePass, identity card and residence permit are all document profiles according to these specifications and use the same technical background infrastructure. This unified approach allows flexibility and rapid responses to political developments such as the current refugee situation.



Since 1 November 2010 the new identity card has been issued in bank card format, with numerous security features that ensure the highest level of protection against forgery.

## eID for eGovernment

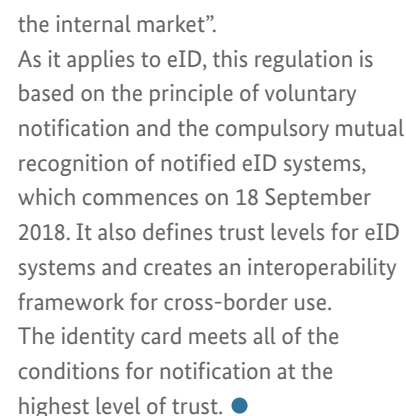
The German federal government has therefore decided, pursuant to its Digital Agenda 2014-2017, to make using the identity cards even simpler and to expand the range of purposes for which their holders can use them. Today, for example, one can use one's identity card to fill in and submit tax returns online (ELSTER) or to easily deregister over the internet any motor vehicle registered on or after 1 January 2015.

optimised at the citizen's end as well. The federal government now offers a second generation of its identity app, the "AusweisApp2". This reflects a strong focus on the ever increasing use of mobile devices. Although not all mobile phones currently in use have the appropriate NFC interface with the necessary range of functions, their numbers are increasing steadily. An additional Bluetooth reader also may serve as a possible alternative.

### Proof of arrival

Due to the large number of asylum seekers who have come to Germany in the last year, the German federal government is working on ways to accelerate the asylum process. On 9 December 2015, the German federal government therefore adopted a bill designed to improve the registration process and the exchange of data for residence and asylum purposes. The purpose of this bill is to ensure that asylum seekers are





Dr Guido Frank,  
Section eID technologies and Smartcards

ital seal) with cryptographically signed data. The security mechanism necessary for this document will facilitate its rapid introduction owing to the fact that it is based on the technical family concept underlying sovereign documents. No new background infrastructure is necessary to read the two-dimensional barcode. For this purpose the established systems already in place for electronic passports and identity cards will be used.

The cross-border use of electronic identities (eID) has undergone some changes as well. In July 2014 the EU adopted Regulation (EU) 910/2014 “on electronic identification and trust services for electronic transactions in







## 25 Years of the BSI

### More security thanks to transparency

*Just as information technology (IT) is a comparatively new technology, the Federal Office for Information Security (BSI) is still a relatively new authority. It was established as a higher federal authority on 1 January 1991, with the BSI Establishment Act of 17 December 1990 as its legal basis and under the German federal minister of the interior division. And just as IT has permeated all governmental, economic and personal activities over the last 25 years and the internet has revolutionised communications, so have the responsibilities of the BSI and the importance of the office also grown.*



### *The beginnings*

Back in the early 1980s, the German federal government and parliament were becoming increasingly aware that the application of information technology also entailed consideration of the necessary level of security and its realisation – and that only a government authority would have the necessary breadth of security information and the ability to guarantee adequate neutrality. Up to that time, security policy was synonymous with territorial defence, and defence in the “cold war” era was interpreted as a matter of intelligence.

By 1986 the Central Office for Encryption (ZfCh), which reported to the Federal Intelligence Service (BND), had been assigned additional responsibilities in the field of “computer security”. In 1989, in response to the expansion of its responsibilities, it was converted into the Central Agency for Security in Information Technology (ZSI). That office has also been a source of recruitment for the BSI, which was newly established by the Act of 17 December 1990 as a division of the Federal Ministry of the Interior.

This gave IT security not only a legal basis, but also a new direction. The Act is based on a new definition of security along with a new understanding of prevention and information policy. As stated in the strategy plan adopted by the German federal government in June 1989: “The federal government will ensure that all concerned and interested parties are informed of risks, precautions and the interaction of different entities (manufacturers, security authorities, users).”

The central idea that a Federal Office

for Information Security should go beyond the protection of state secrets and work to advance IT security in an advisory and supporting capacity for all social groups was not at all self-evident at the time. “The agency that was the forerunner of the BSI worked exclusively in the field of state security”, recalls BSI founding president Dr Otto Leiberich (d. 2015). “The BSI Act then added IT security for the business world and private users to its tasks. Taking on this task was a major challenge.” The BSI will be working from now on in an operational capacity for the government, in a cooperative capacity for the business community, and in an informational capacity for citizens.

### *Responsibilities*

With use of the internet becoming widespread in 1993, if not before, it became clear how prescient this approach was. The increasing digitalisation of the entire society “gave rise to completely new threats of concern to the state, society, business enterprises and the individual” says Dr Dirk Henze, President of BSI, as he recalls those years of digital revolution (1993 – 2002). The security that the business world and government needed for their IT systems in order to function properly became increasingly important. At the same time, the issue of “IT security” became a matter of alarm for an ever broader segment of the public, not least because of breakdowns and failures encountered in the use of online services and the dissemination of malware such as the “Millennium Bug” or the “Love Letter” virus.

IT security had now become a priority government responsibility. To provide and promote it and combat and mitigate the threats facing it, the state must also devote ever greater attention to preventive measures in the civil sector, create the necessary environment, set standards and provide active assistance. “Computer technology is used everywhere today, in both commercial and government processes,” according to Dr Udo Helmbrecht, President of the BSI from 2003 to 2009. “The state must therefore assume responsibility for IT security as well.”

This observation was neither self-evident at the time nor shared by all segments of society. Since its inception the BSI has been at the centre of the discussion concerning the original role of government in the field of IT security and the fine line between conducting surveillance and safeguarding security. As a result, it is undergoing a continual process of development beyond its traditional responsibilities as it transforms itself into an independent and neutral authority for IT security issues in the information society. The BSI sees itself not only as a competent authority for IT security matters, but also as an institution whose actions and leadership merit confidence, not only on the part of the government and government authorities, but also on the part of the public and citizens. This makes it unique as a public authority in comparison to other European institutions.



### *The provider of IT security services*

As a national security authority, the BSI has as its goal to advance IT security in Germany. It functions primarily as the federal government's central provider of IT security services. In that capacity it has operated since 1994 a Computer Emergency Response Team (CERT) which collects and analyses information on vulnerabilities and new attack patterns and relays information and warnings to the affected entities. This is the operational implementation of its awareness of the importance, not only of defending against malware and identifying vulnerabilities, but also of responding to IT security incidents.

But the services provided by the BSI are increasingly aimed at producers along with commercial users and suppliers of information technology. With its IT-Grundschatz, Common Criteria certification and technical guidelines, it is helping to increase understanding of IT security and IT security levels in the private sector as well.

Close cooperation with all parties in the IT and internet sector in the field of IT security is a priority concern for the BSI. The office is represented on the advisory board of the association "Deutschland sicher im Netz e.V.", and it supports the Anti-Botnet Advisory Centre of eco-Verband der deutschen Internetwirtschaft e.V. The same is true in regard to the "Alliance for Cyber-Security", established in 2012 jointly with Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM), in which 1473 institutions, more than 93 active partners and more than 41 information disseminators are currently cooperating on a voluntary basis. Since

2007 the BSI and operators of critical infrastructures in Germany have been working closely together on the basis of the CIP Implementation Plan to discuss new threats and strategies and to implement various measures.

Another concern is educating and increasing awareness among private IT users in matters of IT security. This is a task that the BSI has been undertaking for many years and with ever new services: the information portal BSI für Bürger, Bürger-CERT (Computer Emergency Response Team for Citizens), the BSI Facebook page and the BSI Service Centre. In addition to pure information on a very broad range of IT security topics, the BSI also provides through these channels concrete recommendations for action.

### *Reform of the BSI Act*

The rapid development of information technology is giving rise to new IT applications in almost every area of everyday life – and with these come ever new security vulnerabilities. This calls for new responses. To meet current IT threats and in recognition of the increasing importance of information and communication technology, the BSI Act was amended in 2009 by the Act to Strengthen the Security of the Federal Government's Information Technology, which finally turned the BSI into a national IT and cyber security authority. "The amendment of the BSI Act in 2009 was an important milestone for the future development of the BSI," observed then BSI President Helmbrecht.

With its expanded powers, the BSI was now able to take on new tasks. It developed for the various federal authorities mandatory security standards for the procurement and use of IT. By taking on the responsibility of protecting the government networks, the BSI became the central notification point for IT security within the federal administration. This arrangement was designed to ensure, through prepared information and competent analyses, the federal government's ability to take the necessary actions and decisions in the event of an IT crisis of national importance. And it established an IT crisis management team for the federal administration as a kind of early warning system that facilitates the creation of situation reports, defines crisis response processes, and conducts exercises in support of those processes.

In addition, the BSI was empowered to take measures to protect against threats to the security of the federal government's information technology. To protect government networks, it is authorised to collect and analyse incoming data on those networks. The analysis process has been automated as much as possible and is subject to strict controls. This gave the BSI the ability to detect and repulse IT attacks on those networks.

When the federal government adopted its Cyber Security Strategy and created a National Cyber Response Center (Cyber-AZ) in 2011, partly in response to the attacks on process control systems by the highly specialised Stuxnet malware, it was obvious that it could do so only in Bonn and under the management of the BSI. On 16





**01/01/1991**

**Founding of the Federal Office for Information Security under Dr Otto Leiberich**

The Federal Office for Information Security commences its work on 01/01/1991 (Act on the Federal Office for Information Security).



**1994  
CERT**

In 1994, the first Computer Emergency Response Team (CERT) is set up in the BSI. Not only was the importance of defending against malware and identifying vulnerabilities recognised, but also of responding to IT security incidents.

**01/08/2001**

**Central provider of IT security services for the Federal Government**

On 1st August 2001, new organisational, staffing and technical framework conditions enter into effect for the ongoing development of BSI to become the central provider of IT security services for the Federal Government.

**01/01/2000**

**Millennium Bug**

The fear of malfunctions, due to the hitherto conventional two-digit data format having to become four-digit after the turn of the millennium, leads to thorough analyses of IT systems in the Federal Administration and considerable preparations in the event of their potential failure. The BSI takes the lead in this matter.



**March 2002**

**BSI für Bürger**

The information service BSI for Citizens launches as a CD-ROM in March 2002 with the slogan 'Ins Internet – mit Sicherheit!' (or 'online and secure!') and becomes available on the internet.

1990

1991

1992

1993

1994

1995

1996

1997

1998

1999

2000

2001

2002

2003

2004



**01/01/1993**

**President Dr Dirk Henze**  
Dr Dirk Henze is appointed.



**1994**

**Introduction of IT-Grundschutz**

Working together with leading business enterprises, the BSI creates and publishes the IT Baseline Protection Manual which subsequently develops into the benchmark for IT security management in Germany.



**04/05/2000**

**'Love Letter' worm**

Malware enters broad public consciousness for the first time: With its enticing subject line ('I love you'), the 'Love-Letter' computer worm spreads by email on a massive scale and causes global damage costing approximately USD 10 billion.



**01/03/2003**

**President Dr Udo Helmbrecht**

After the end of Dr Dirk Henze's term in November 2002, Dr Udo Helmbrecht is appointed BSI President in March 2003.

**01/11/2005**

**Electronic passport**

The newly introduced electronic passport is fitted with an integrated radio frequency chip that stores the facial image and personal data, as well as fingerprints since 01/11/2007. The BSI develops corresponding protocols and technical guidelines to support the security objectives pursued with the electronic passport: data privacy, authenticity and counterfeit protection.

**20/08/2009****Amendment of the BSI Act**

The Act on Strengthening IT Security in Federal Information Technology enters into force. The Act, inter alia, states that the BSI is able to pass on information and warnings regarding security issues in IT products and services as well as those relating to malware to the bodies concerned or the general public. In particular, however, the BSI now becomes the central reporting body for the IT security of federal authorities and hence responsible for safeguarding the IT security of the Federal Government.

**16/10/2009**

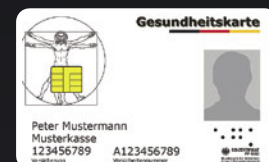
**President Michael Hange**  
Michael Hange is appointed President of the BSI.

**01/10/2011****Electronic health card**

The legislature ruled on the introduction of the electronic health card (eGK) with the healthcare reform of 2004. Since 1st October 2011, health insurance funds have gradually begun issuing their policy holders with the new card. The technical guidelines of the Federal Office for Information Security (BSI) as well as the safeguarding of IT security and reliability of technical components, through certification according to defined protection profiles, provide an important contribution to the high security standard of the electronic health card.

**01/04/2011****National Cyber Response Centre:**

The National Cyber Response Centre in Bonn commences its work. Under the leadership of the BSI, the National Cyber Defence Centre serves as a common platform for fast information exchange and better coordination of protective and defensive measures in the event of IT security incidents.

**23/02/2011****Cyber security strategy**

The Federal Cabinet determines the cyber security strategy for Germany.

**18/02/2016**

**President Arne Schönbohm**  
Arne Schönbohm is appointed President of the BSI.



2005

2006

2007

2008

2009

2010

2011

2012

2013

2014

2015

2016

2017

2018

**01/11/2010****Electronic ID card**

The new electronic identity card makes it possible to securely and conveniently verify one's identity to authorised companies and public agencies online. The BSI establishes the necessary security standards and ensures the quality of the technical processes.

**June 2010****Stuxnet**

Stuxnet is the first known malware program to specialise in the process control system. This brings the vulnerability of industrial systems and critical infrastructures into focus.

**06/06/2013****NSA scandal**

*The Washington Post* and *The Guardian* publish secret documents that prove American and British security services monitor global telecommunications, and particularly the internet, on an unprecedented scale. It then becomes evident that top-level German politicians were also spied upon. The 'NSA scandal' triggered by this provokes a number of political discussions on cyber security and the practises of secret services.

**July 2007****Zeus**

The Zeus Trojan horse malware is first detected: it is primarily used to spy on personal and financial data. It ranks as one of the most 'successful' Trojan horses to this day and has infected millions of PCs in its various forms.

**08/11/2012****Allianz für Cyber-Sicherheit**

In cooperation with Bitkom ('Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.'), the BSI establishes the Allianz für Cyber-Sicherheit. The alliance is an association of all the key players in cyber protection in Germany which seeks to increase cyber protection in the country.

**25/07/2015****IT Security Act**

An extensive supplement to the BSI Act in the form of the 'Act to Increase the Security of Information Technology Systems (IT Security Act)' enters into force. It puts emphasis on strengthening the IT security of operators of critical infrastructures.



June 2011, the National Cyber Defence Centre was launched on the premises of the BSI as a common platform for fast information exchange and better coordination of protective and defensive measures in the event of IT security incidents. Staff from the BSI, the Federal Office for the Protection of the Constitution (BfV) and the Federal Office for Civil Protection and Disaster Assistance were recruited; since June 2011, the Federal Criminal Police Office (BKA), the Federal Police, the customs office, the Federal Intelligence Service (BND) and the Bundeswehr have been providing assistance as associated agencies.

### *Work on projects*

The potential of IT and the opportunities it affords are realised only when there is confidence in the security of the technology. The assurance of qualified authorities and established IT security standards provide the foundation on which this trust is built. With its focus on IT security standards, the BSI is always becoming involved in pioneering projects such as those concerned with smart meters or cloud computing. In the field of smart meters, the BSI has worked with the business community and data and consumer protection advocates to come up with a common protection profile and technical guidelines. It has also worked with manufacturers to formulate minimum security requirements for cloud computing, which it published in a benchmark paper. Great importance is attached also to assisting and participating in socially relevant projects that affect citizens in their daily lives, such as De-Mail and the new identity card. The main security objectives of confidentiality, integrity and authenticity in the

De-Mail communication system are guaranteed through defined security measures to which BSI has made a decisive contribution. Since November 2010 the new identity card has not only put citizens in possession of a picture ID in a new bank card format, it also provides additional electronic functions that significantly enhance security even on the internet. These include the electronic identity document and qualified electronic signatures.

### *Critical infrastructures*

A special point of focus in cooperative efforts with the business community is the protection of critical infrastructures, a responsibility shared jointly by the operators of such structures and the State. This got a boost with passage in July 2015 of the IT Security Act, which once again expanded the duties and responsibilities of the BSI. "This law puts the BSI in the role of central authority for IT security matters affecting the business community and society at large," says former BSI President Michael Hange (2009 - 2015). "And it can now make its contribution to securing the critical infrastructure on a secure legal basis." Because critical infrastructures are indispensable to the common good and are becoming increasingly dependent on IT, they will be expected in future to maintain a minimum level of IT security and to report IT security incidents to the BSI – just like the Federal Administration. For its part, the BSI must gather all information relevant to defence against attacks on the IT security of critical infrastructures, evaluate it, and refer it to the operators of those infrastructures and to the competent (supervisory) authorities. In so doing, the BSI will be assuming for the operators of critical infrastruc-

tures the same role it assumed for the various federal authorities in 2009. The collaborative approach embodied in the law allows not only the government and the business community to benefit from each other's expertise, it also best serves the task of ensuring the highest possible level of IT security for society as a whole.

Conclusion: The BSI has evolved over the last 25 years into an operationally active authority that is responsible at the national level to the business community, the State, and society at large for the security of information, a responsibility that it exercises with authority in all areas of IT security. But the extensive list of its responsibilities and its powers as provided in the BSI Act rightly create high expectations that the BSI will meet future challenges as it has since its inception: with success. ●

## 25 Years of the BSI Act - The Development of Responsibilities and Powers

### 1991: Act on the Federal Office for Information Security

With the relevance of security of IT systems to the proper functioning of business and government becoming ever more important even as it faced ever greater threats, the government was forced to expand its role, once limited to approving products for processing and transferring classified material, to one that included the ability to take measures to minimise such threats.

The newly established BSI was designed to make a public contribution to the promotion of IT security by investigating security risks, developing safety precautions and issuing security certificates. Its responsibilities also included developing appropriate test criteria for systems and components, and advising manufacturers, vendors and users of information technology systems and components. In addition, it was to make its expertise in information technology available to law enforcement and domestic intelligence agencies to enhance their ability to combat the rising incidence of cyber-crime.

The “Act for the Establishment of the Federal Office for Security in Information Technology” was in effect from 1 January 1991 to 19 August 2009.

### 2009: Act to Strengthen the Security of Federal Information Technology

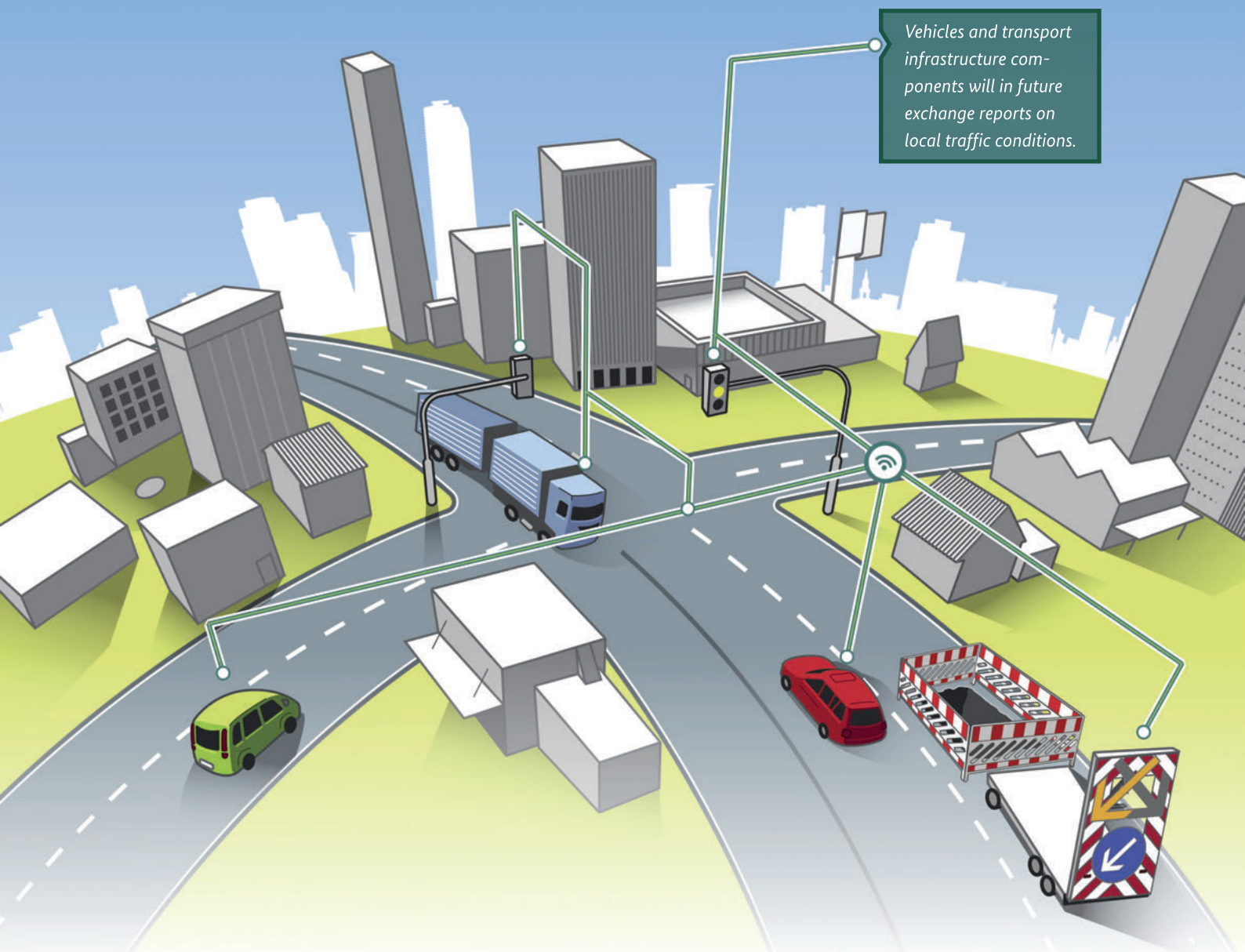
One of the key provisions in the amendment of 2009 (“Act to Strengthen the Security of Federal Information Technology”) established the BSI as the central authority responsible for ensuring the security of the federal government’s information technology. When the law went into effect on 20 August 2009, the BSI became the central notification point for federal agencies on matters of IT security. Since then it collects information on security vulnerabilities and new attack methods that threaten the security of information technology, analyses them and issues situation reports. This gives it the ability to detect attacks on the federal government early and to take prompt countermeasures. The BSI may also bring warnings to the attention of concerned parties outside the federal government or to the attention of the public at large.

In addition to its ability to develop technical guidelines for the security of information technology in the federal administration, the BSI was also empowered to take measures to protect against threats to the security of information technology in the Federal Republic. To protect government networks, the BSI is therefore allowed to collect and analyse incoming data from those networks. This puts it in a position to detect and avert IT attacks on those networks.

### 2015: Supplementation by the IT Security Act.

Because of the potential for threats to spread rapidly from conventional IT systems to industrial systems, the 2015 amendment (“Act to Increase the Security of Information Technology Systems”) placed particular emphasis on strengthening IT security for operators of critical infrastructures. Because they are equally indispensable for the common good and ever more dependent on IT, in future they are to maintain a minimum level of IT security and report IT security incidents to the BSI. For its part, the BSI collects all information relevant to defence against attacks on the IT security of critical infrastructures. This information is evaluated and referred to the operators and to the competent (supervisory) authorities.

As a result of the law that went into effect on 25 July 2015, the BSI will assume for the operators of critical infrastructures the same role it assumed in 2009 for federal agencies.



Vehicles and transport infrastructure components will in future exchange reports on local traffic conditions.

# Right of way for IT security

## Intelligent transport systems

All across Europe the course is being set for automated driving. At the end of April 2016, an important clause in the 1968 Vienna Convention that prohibited the use of autonomous driving functions will cease to apply. In the past, according to the Convention for the Unification of Traffic Rules, a driver was required to drive his car himself at all times and was therefore not allowed to take his hands away from the steering wheel. Legislation is

now being brought forward that would permit manufacturers and suppliers to install assistance systems capable of independently steering a vehicle, keeping to or changing lanes, and braking in an emergency. The only requirement will continue to be that the driver always be able to override the assistance systems and take control. It is now up to the manufacturers and suppliers to convince future customers of the reliability of the already highly developed

assistance systems. It won't be long before there is an evasion manoeuvring system in addition to the already familiar emergency braking systems, which has pedestrian detection capabilities. The first system to be introduced will presumably be the autobahn assistant, which will independently keep a vehicle to a lane within specified speed ranges and take complete control of the vehicle's brakes in dangerous situations.





***In a mere ten years your ride home from the office could look like this:***

Through a service app on his smartphone, the driver has specified the route he plans to travel in the evening. He had left his car that morning at the parking garage located in the immediate vicinity of his office. His vehicle's piloted parking technology has relieved him of the need to search for a parking space himself. The vehicle now takes care of that independently. The considerable amount of time he once had to devote to the tedious process of finding a parking space can now be used for work.

The position-sensing function of his service app tells the vehicle ahead of time when the driver will be arriving at the agreed check-out point at the parking garage. The e-vehicle, which has automatically charged up through induction surfaces while parked, arrives at the check-out point to meet him.



For the trip into the city, the driver has decided to steer the vehicle himself. It is only once he is on the motorway that he will relax and let go of the steering wheel. The traffic signs, which for the last few years have been equipped with intelligent communication modules, help him by supplying information on the traffic situation, information that is transferred to him in his

vehicle in real time. How easy it has now become to find the fastest route out of the city! It is hard to believe that just a few years ago road traffic was still controlled largely with static information. Once on the motorway, the driver flips a switch to activate the autopilot. A message appearing on the vehicle's central display unit tells him that all of the autopilot's functions are available and working flawlessly. He presses a button on the steering wheel to confirm that he has transferred the steering function to the autopilot.

All systems in the vehicle are working now, and short-range radar, a front-mounted camera, and long-range laser or radar technology are being used to create an exact image of traffic events. The position data from the Galileo satellites, which are accurate to the metre, and the sensors' comparisons with fixed objects filed in the navigation system, such as guard rails, buildings, traffic lights and curbs along the route, enable the vehicle to determine its travel position on its own and with an accuracy to the centimetre. All of these fixed landscape objects are stored as data in the new high-precision road and landscape maps in the vehicle's navigation system.

***Reaching your destination safely and relaxed.***

According to plans formulated by the automotive industry, automation of vehicle guidance systems is expected to develop incrementally until 2030, proceeding from partial automation to a high level of automation, then to full automation and, ultimately, to the development of driverless, autonomous vehicles.

But until the time arrives when all vehicles are controlled without a driver, there will always be situations that a vehicle will not be able to negotiate on its own. Dangerous situations may arise, for example, in the wake of an accident or during a snowstorm. If lanes can no longer be perceived with certainty, the system will transfer control to the driver with a timely warning signal.

***Detecting hazards before they become a threat.***

Current developments towards a networked automobile constitute another important element in the development of automated vehicles. Such vehicles will be able to exchange current traffic information by radio, initially amongst themselves and, soon thereafter, with transportation infrastructure components such as road signs or traffic signals (roadside units). The first case is referred to as vehicle-to-vehicle communication, the second as vehicle-to-infrastructure communication. Both are grouped under the term 'vehicle-to-X communication'. The timely dispatch of traffic-related information will enable drivers to avoid congestion and accident sites. If a vehicle travelling up ahead ends up in a traffic jam or is forced to brake for other reasons, a data packet with this information

will be sent to the vehicles behind it so that their driving behaviour can be (automatically) adjusted accordingly. The aim of this sort of exchange is to provide the vehicle driver with timely information before he perceives the situation on his own. In future, this information will also be used to support automated driving. In contrast to the autonomously travelling car, vehicles that operate with a network system will soon be appearing on the market.

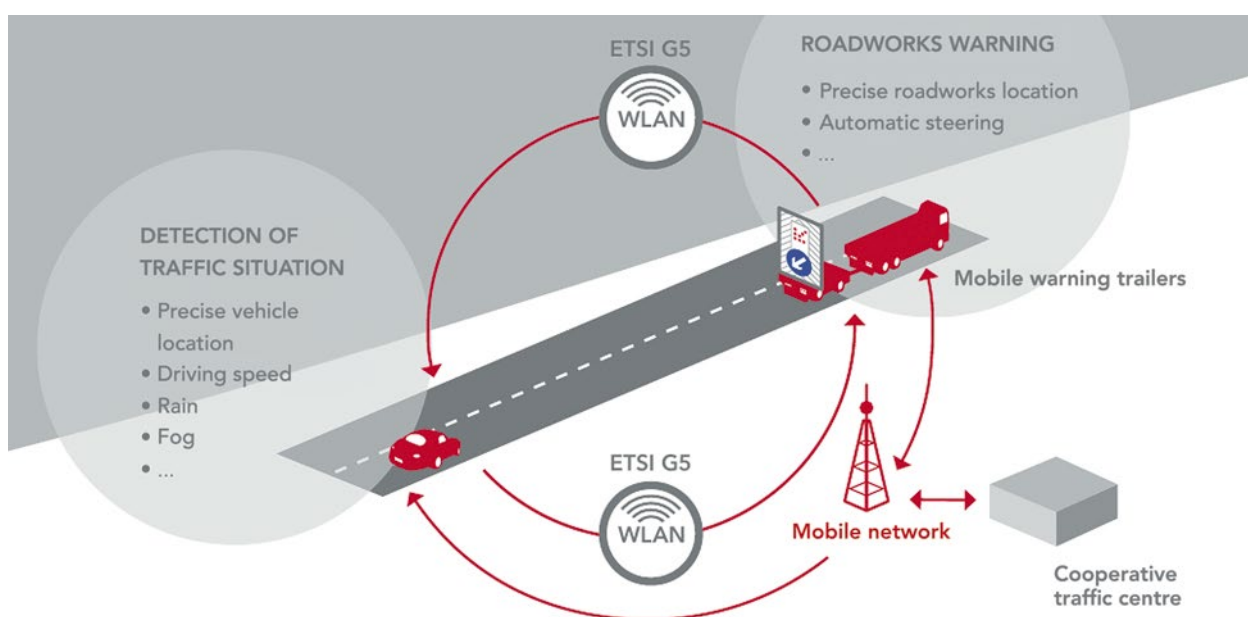
With the new communication capabilities, however, vehicles that have operated in the past as closed systems will be “opened” to the outside world and thereby become exposed to possible abuse by potential attackers. Certain vehicles are already externally vulnerable to hacker attacks through their interfaces, as numerous published articles have recently shown. It was possible in one case, for example, to interfere with the steering of a moving car through a mobile telephone connection.

Even vehicle-to-X communication is conceivably vulnerable to attack; for example, in heavy freeway traffic, a

malicious attacker could disseminate the false message that certain vehicles are slamming on their brakes, thereby inducing vehicles behind them to engage in dangerous braking maneuvers. Or an attacker in proximity to a construction site could send out reports that the left lane is closed when it is actually the right lane that is blocked. This could provoke traffic tie-ups or even accidents. Such opportunities for attacks must therefore be prevented; in particular, the integrity and authenticity of the messages that are exchanged must be ensured through appropriate procedures. To secure communications between vehicles and traffic control centres, the BSI is therefore promoting the development of an IT security plan for infrastructure components.

The Federal Government is promoting the topic of vehicle networking with its commitment to building an intelligent transportation infrastructure. An early application project in which use is made of vehicle-to-X communication is the C-ITS Corridor project. The C-ITS Corridor was initiated in 2013 as a transnational project of the German, Dutch and Austrian Ministries

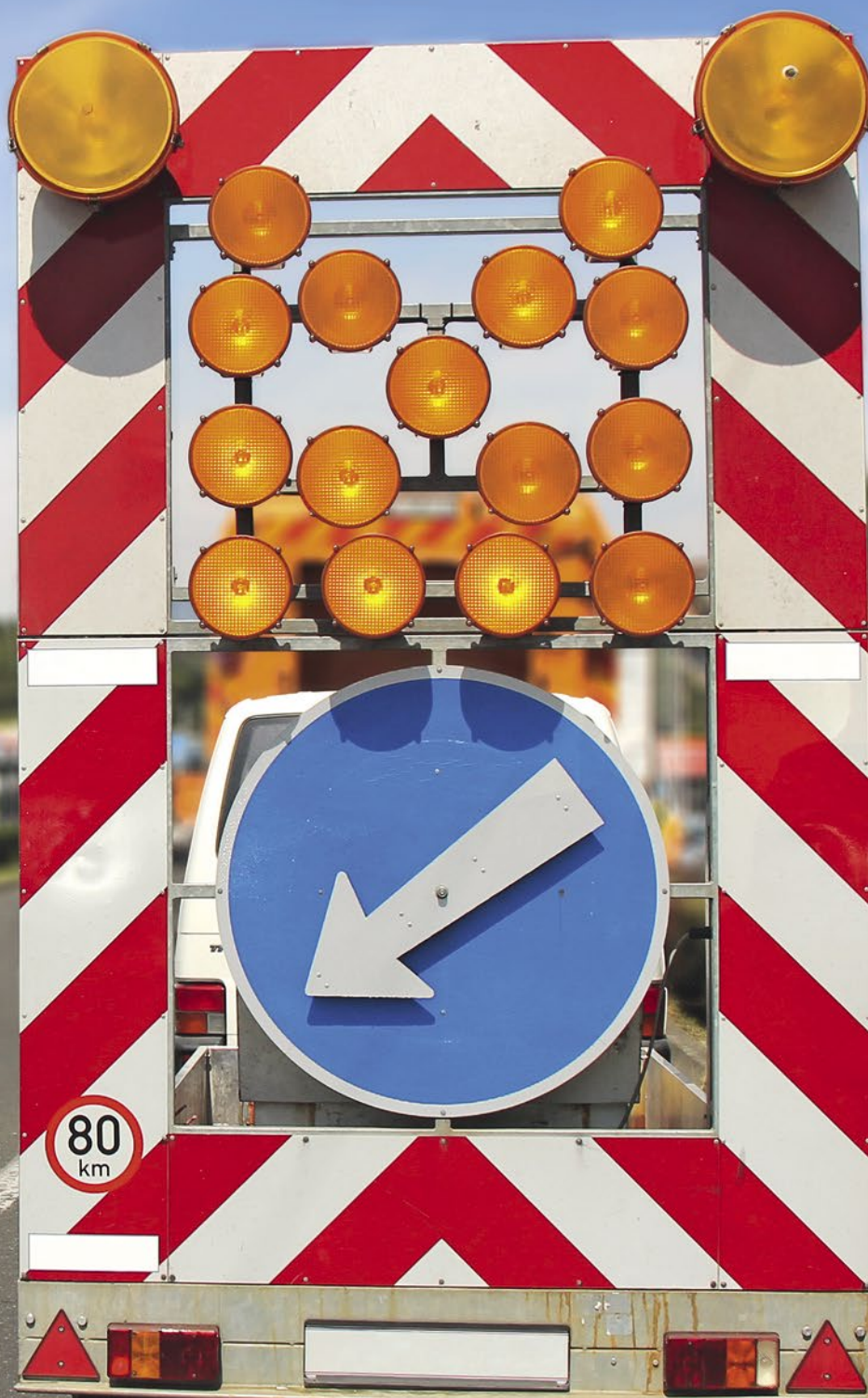
of Transport. This project includes a plan to equip an autobahn corridor from Rotterdam to Vienna via Frankfurt am Main with initial intelligent transportation systems that make use of vehicle-to-X communication. Two services will be implemented: A construction warning system and traffic monitoring (see illustration). A key role will be played by construction site warning trailers, which are used for temporary roadwork sites and maintenance measures. The construction site warning units will be equipped with the appropriate gateways for communicating with vehicles. Car models appearing on the market in the future will be equipped with suitable communication components as well. As such vehicles approach a construction site, they will receive alerts through the gateway along with information on closed lanes and speed limits that will appear on a display inside the vehicle. This will give the driver time to adjust his driving behaviour. Another function will enable vehicles themselves to send messages describing their current state (current speed, direction, etc.) or their immediate environment (e.g. weather conditions). These will be received



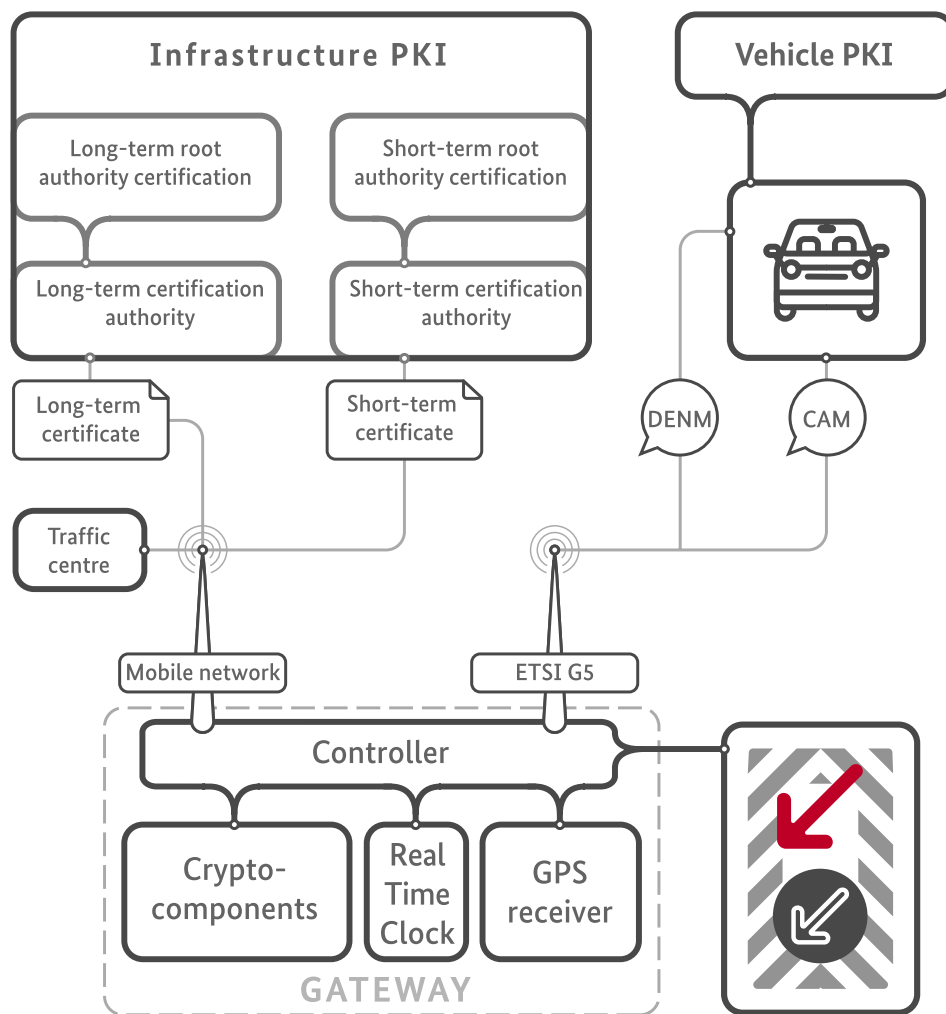
*The two services of traffic monitoring and construction site warning in the C-ITS Corridor. Data are transmitted over a Wi-Fi-based channel (ETSI G5).*



*Initial application projects: In the future, construction site motorways, for example, will be equipped with gateways. Information about such things as closed lanes, speed limits, or the speed at which traffic is currently moving will be exchanged over the data connection between vehicle and warning sign.*







PKI structure for the gateway of a construction site warning sign. Long- and short-term certificates are issued by various certification authorities. These authorities are in turn each connected to a dedicated root certification authority. The gateway exchanges cooperative awareness messages (CAM) and decentralized environmental notification messages (DENM) with the vehicles. CAMs are sent at short intervals and contain information on the current state of the vehicle, such as its speed and direction of travel. DENMs are equivalent to alerts and are transmitted only in special traffic situations, including those associated with the construction sites themselves.

by the site warning unit gateway and relayed to a traffic control centre, where the information will be used in combination with data sources that are already available to prepare traffic situation reports.

The wireless network protocol that is used and the message formats for vehicle-to-X communication have been standardized by the European Tele-

communications Standards Institute (ETSI). The ETSI specifications also require that message packets be digitally signed to ensure their integrity and authenticity. Some of the signatures used are based on elliptical curves (ECDSA). For this, a suitable public key infrastructure (PKI) must be built that issues and manages the certificates for the signature keys which are used for the vehicles and the construction

site motorways. The German Federal Ministry of Transport and Digital Infrastructure, which is responsible for the project, got the BSI involved early on in designing the PKI for transportation infrastructure components such as construction site motorways. The currently developed concept is based on two types of certificates: long-term and short-term certificates (credential certificates). Immediately after it is pro-

duced, the gateway in the construction site motorway will be equipped with a long-term certificate that will be valid for several years. Before each planned use (such as on temporary construction sites), a short-term certificate will be requested whose validity period will cover the duration of the construction. The long-term certificate will be used for authentication of the short-term certificates by the authentication authority. The key associated with the short-term certificate will be used to sign the alerts sent by the gateway. Its short validity period reduces the potential for attacks in the event that the gateway is compromised, and a costly revocation test of the sort that would be necessary for certificates with longer validity periods (i.e., a test to determine whether a certificate has been invalidated) is avoided at the vehicle end.

A dedicated PKI will exist for the signature key used at the vehicle end. It must of course be ensured that vehicles and transportation infrastructure components are able to verify each received signature or certificate. For this to happen, each party must have access to the public key of the other party's root certification authority.

The PKI as outlined above results in a complex key management system. As a component responsible for cryptographically ensuring the authenticity of alerts with an impact on traffic, the gateway on the construction site motorway is in great need of protection. An attacker, for example, must not be able to find a way to read out the private signature key for the gateway's outgoing messages. A suitable hardware component must therefore be used that permits secure storage of private key material. Potential attackers must also be prevented from altering the behaviour of the gateways by,

for example, manipulating software or firmware. In cooperation with the Federal Highway Research Institute (BAST), a protection profile describing the requirements for the gateway is currently being created according to common criteria.

Networked travel will of course not be limited to Germany. Since networking functions must be useable across borders, the systems used must be harmonised internationally. To this end the European Commission has created the C-ITS platform, in which experts in various working groups have developed recommendations for the deployment of intelligent transport systems at the European level. These call for close international coordination in the field of IT security, as it is to be assumed that national public key infrastructures will continue to exist, and these must be interoperable.

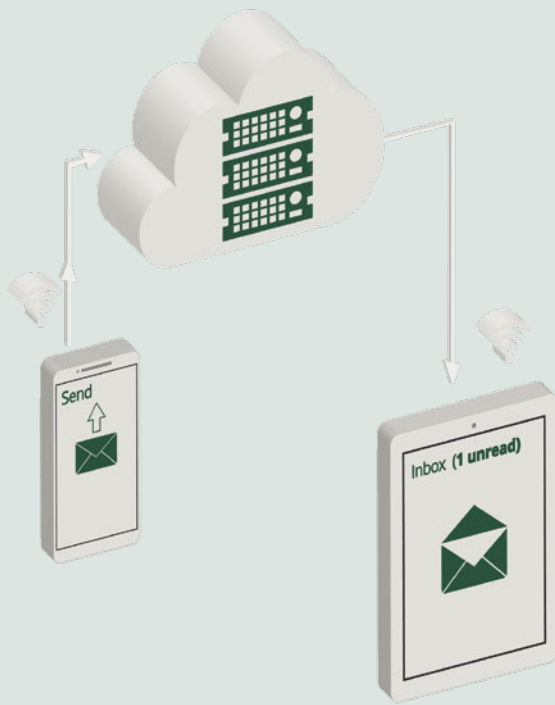
Networked and autonomous travel will significantly change the nature of road traffic in the next several years. As we have seen, car-to-X communication will not remain limited to interactions with construction site motorways. Networked vehicles will penetrate further into the market, and more transportation infrastructure components will be added all over the country. IT security is becoming increasingly important, and even more attention will have to be given in future to securing the hardware used in vehicles and roadside units and to protecting against hacking attacks. The concept outlined above provides a foundation for secure message exchange and trustworthy transportation services that will also support future use in the service of automated travel. ●



*Christian Wieschebrink,  
Section Technological Fundamentals of eIDs  
and Chip Security*



*Hans-Peter Wagner,  
Section Technological Fundamentals of eIDs  
and Chip Security*



# Secure communication in the digital age

## With an application-oriented combination of measures in practice

E-mail remains an important medium for exchanging messages in digital communication, despite the growing importance of mobile instant messengers. As a rule, e-mail messages continue to be sent without consistent application of IT security measures such as encryption or digital signatures. In contrast to closed systems, this reflects the heterogeneity of the globally networked IT landscape used to transmit e-mail.

With its planned technical guideline “Secure E-Mail Transport” (BSI TR-03108), the BSI has set out to define a minimum standard for IT security measures for the transport of e-mail and to thereby contribute to the further propagation of secure e-mail technologies. This project supplements De-Mail and various projects to promote end-to-end security of digital communication. The measures called for in the

technical guideline are distinguished primarily by the fact that they work without the user’s active participation.

The need for transparent secure e-mail transport was recognised by e-mail service providers (EMSP) early on and addressed in the marketplace. In addition, various market participants have expressed the wish that the BSI would create a standard for that purpose. In preliminary discussions, possible organisational and technological concepts were discussed. Ideas were developed, discarded or modified and developed further. The end result was a viable concept with concrete requirements for EMSP that were conceived to generate a gain in security for all participants in the e-mail infrastructure. To that end, the technical guidelines define minimum requirements for the operation, systems, and interfaces of an

EMSP. Compliance with these minimum requirements will ultimately benefit not only the users of the EMSP, but also users of other providers, since the messages that are sent will be transmitted over secure connections.

### *Field-tested approaches*

This added value is the result primarily of consistent use of established standards. In addition to the BSI’s own standards, such as its technical guidelines for cryptographic standards for projects of the Federal Government and for secure operation of certification authorities, international standards also play an important role in this connection.

The use of DNS-based Authentication of Named Entities (DANE) has been especially well received by the public. This relatively new internet standard enables internet service providers to make known their certificates, which are needed for authentication and encryption, through publication on DNS servers. In the analogue world this is comparable to leaving public keys in a phone book. In this manner anyone wishing to make contact with a service provider can do so by encrypted means. DANE actually goes a step further at this point, as its use is at the same time a statement that the service provider is by default able to offer an encrypted connection. DANE is therefore a technology that by necessity makes secure connections generally available in a scalable manner. The BSI itself already offers, and has for some time, its services on the internet with DANE. In contrast to DANE, internet connections that are secured using Transport Layer Security (TLS) have for some time been seeing increasingly widespread use in practice. Security vulnerabilities to such threats as the Beast trojan or the Poodle “man-in-the-middle attack” have recently shown that the use of



up-to-date encryption procedures is of essential importance. For this reason the BSI publishes annually, and as the occasion warrants, new safety standards, which are applied also for secure e-mail transport. Combining the DNSSEC internet standard for secure querying of DNS servers, DANE for retrieval of certificate information, and the use of secure algorithms for TLS, a uniformly high level of security can be achieved with the aid of standard technologies.

Defining only the requirements for the interfaces is, however, not enough to secure from point to point the entire route an e-mail message travels from sender to recipient. Each EMSP constitutes a point in the infrastructure that, depending on the route an e-mail message takes, processes that e-mail along its path. An EMSP therefore also needs to operate securely. For this reason the technical guidelines formulate requirements for the security concept the EMSP is required to create. When it is combined with the stringent data protection requirements that apply

to the operation of an e-mail service, the entire route an e-mail message travels between sender and recipient is covered.

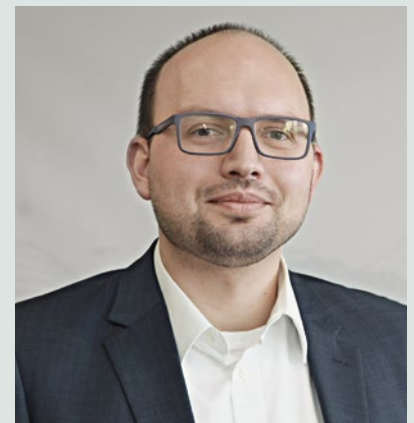
Every e-mail service provider is to be given in future the opportunity to prove that its service conforms to the technical guidelines for purposes of a certification procedure. An appropriate certification scheme is currently under development. Through the certification process, the service provider receives from an independent authority proof that it has implemented a defined level of security. This serves to distinguish it from other market participants, but it also provides transparency for its users.

In contrast to these comprehensive or cross-system measures, which serve to create a comparable level of safety in an open infrastructure, other projects such as De-Mail create closed infrastructures. These allow concrete statements regarding the safety level of every message sent over this infrastructure. This enables the creation of obligations that permit digital communication and which, under certain conditions, conform even to the standards that are suitable for replacing conventional written form. The two projects thus cover complementary application areas.

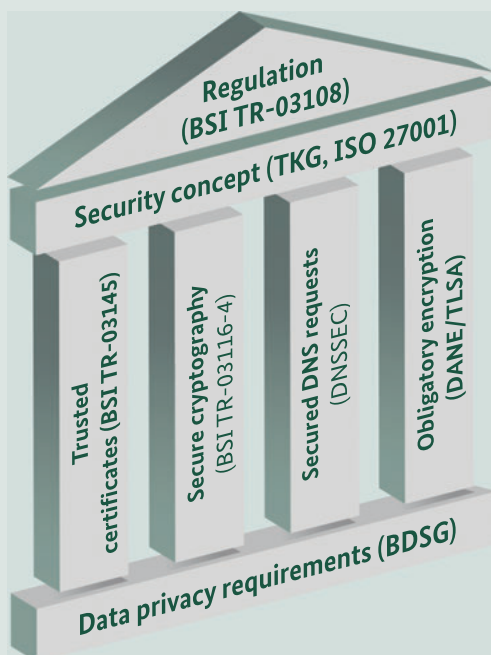
Irrespective of the infrastructure used to transport a message, the BSI is actively promoting projects to implement security end to end. These procedures are not yet in widespread use. One reason for this may be a perception that they are insufficiently user-friendly as a result of, for example, a key management system that is usually complex and time-consuming. Current projects start at precisely this point and aim to provide users with a procedure that is as automated and as user-friendly as possible. Both De-Mail and regular e-mail can now be transmitted securely from end to end in a significantly simplified

manner, thereby achieving a visibly high level of confidentiality for the user.

Ultimately, it is not only the combination of measures within a project that determines the success of secure digital communication, but also the interaction of projects that are complementary in their application. ●



Florian Bierhoff,  
Section Secure eID Applications



Conceptual overview  
of requirements

# The new president of the BSI

## Arne Schönbohm takes office

*With former BSI President Michael Hange going into retirement, Federal Interior Minister Thomas de Maizière announced on 11 December 2015 that he would propose Arne Schönbohm, at that time president of Cyber-Sicherheitsrat e.V., as future president of the BSI. Upon confirmation by the Federal Cabinet, Schönbohm took up his new position on 18 February 2016.*

Prior to his appointment as BSI president, Arne Schönbohm served for more than three years as president of Cyber-Sicherheitsrat Deutschland e.V., which had been established in August 2012. The Berlin-based association is politically neutral and has set itself the task of advising companies, public authorities and policymakers on matters of cyber security and strengthening them for the fight against cybercrime. Members of the association include large- and medium-sized business enterprises, operators of critical infrastructures (KRITIS), German states, municipalities, and experts and policy makers in the field of cyber security.

In addition to this activity, Arne Schönbohm served, beginning in late 2008, as CEO of BSS BuCET Shared Services AG (BSS AG), which advises companies and public authorities in the fields of digitalisation, cyber security and data protection. The portfolio of BSS AG also includes consulting services in the fields of public affairs and public relations intended to communicate digital topics and messages in a professional and expert manner. In both capacities, Arne Schönbohm has, as an expert and speaker who is in demand nationally and internationally, expressed his views in numerous publications and media appearances on the topics of cyber crime and cyber security.

He has given special attention to networking and consulting at the decision-making level as a key point in the fight for global cyber security. Arne Schönbohm has appeared in the U.S.A., among other places, as a speaker at events held by the National Association of Corporate Directors (NACD), and as an expert witness at hearings in the parliament of North Rhine-Westphalia and the Berlin House of Representatives. He is also the author of various books, including *Deutschlands Sicherheit - Cybercrime und Cyberwar* (2011).

Born in Hamburg, Arne Schönbohm (born 1969) graduated from the Gymnasium Röttgen in the Rhineland in 1989. Following his military service, he studied international business administration at the International School of Management in Dortmund, as well as in London and Taipei, earning his diploma in Business Administration in 1995.

Schönbohm began his 13-year career in industry as a trainee in the central group of junior staff at DaimlerChrysler Aerospace in Munich. At the end of his training period, he worked as a clerk in the strategic corporate development department of Motoren- und Turbinen-Union (MTU) and



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

as head of the executive office. Following the formation of the European Aeronautic Defence and Space Company (EADS), he left in September 2001 to work for EADS Defence and Civil Systems, where he served as Senior Manager Telecom. In 2003, as a member of the management for the Public Affairs and Homeland Security departments at EADS Telecom Germany GmbH, he moved to Ulm. In 2005 Schönbohm returned to Munich, where he assumed responsibility for strategy and business development for EADS Secure Networks and served as a board member. In 2006 he rose to the position of Vice President for Commercial and Defence Solutions. There he was responsible for developing and managing this international business segment and acquired, in particular, the armed forces and critical infrastructure operators such as utilities, airports and local public transport authorities as customers for EADS Secure Networks. Schönbohm has been a member of the Cyber Security Coordination Group since December 2012. ●

# Invitation to the workshop

## New format of media dialogue

*Those who hope to interest journalists in their work must be able to offer them something. This should be first and foremost content that is useful and significant, though the form in which it is presented also plays a role. The BSI has therefore introduced the new "workshop discussion" format for its relations with the media. This enables journalists to acquire a deeper insight into the work of the BSI, become acquainted with both people and products, and bring up questions of a technical nature in discussions. This format was first successfully implemented on 29 October 2015.*

As a national IT and cyber security authority, the BSI is responsible for protecting the voice and e-mail communications of the Government and Federal Administration by means of cryptography and secure devices. This includes providing, in cooperation with various manufacturers, communications solutions for use in the Federal Administration and creating an awareness therein of the importance of their use.

For this reason, a call for tenders was issued in 2012 for secure mobile communication devices for the Federal Administration. The BSI was responsible for defining the requirements, approving selected devices, and providing a communication platform for the exchange of experience. For the BSI and the manufacturers, this tender was associated with the challenge of finding a compromise between security, usability and price that would satisfy all parties.

Encryption is applied counterintelligence. From a journalistic perspective, this makes it more than an arcane IT-specific topic. And rightly so, as it concerns the protection of government communications. But secure mobile communication is also an issue that journalists are keen to pursue as a matter of their own self-interest. For journalistic investigation and robust protection of informants are inseparably dependent on the ability to communicate securely through mobile devices.

Cryptography is a complex technical field to which journalistic coverage does not exactly bring clarity, especially when those dealing with it are not journalists with a specialisation in IT but politics and society page editors. The workshop discussions are therefore intended to convey to journalists what BSI means by cryptography and which cryptographic solutions are available and best suited to different communication, applications, and user groups. For this reason, Dr Gerhard Schabhüser, department head for cryptographic technology in the BSI; Dr Uwe Kraus, department head for VS-IT security, standards for and approvals of cryptographic systems in the BSI, and Clemens Taube, BSI speaker on the topic of cryptography in applications, made themselves available as expert interlocutors.

Following a keynote speech by Dr Schabhüser on the elements and basic objectives of cryptography, types of encryption, and key management and distribution, Dr Kraus spoke about the technical guideline "Cryptographic

Methods" and presented various cryptographic solutions. The journalists asked numerous questions concerning both political and technical aspects of the subject. This illustrates that, even for journalists, it is not only the technical aspects but also the users' perspective that play an important role. The question as to what is technically feasible was given no more weight than the question as to how the technically feasible figures into everyday professional activities. And that is how it should be, for an exact congruence of both perspectives is crucial to the success of the security measures that are employed. And not just at federal authorities, but also in the business world and the media. After this successful start, the BSI's workshop discussions with journalists are to be continued in 2016. ●





# Innovative and yet still relevant to everyday life

## The BSI as an employer

*Thomas Gilles works as a specialist advisor for secure eID applications at the BSI. In the following interview, he talks about how he started work at the BSI while studying for his bachelor's degree, and why he chose a career in the civil service.*



*Thomas Gilles,  
Section Secure eID-Applications*

### **How long have you been working at the BSI and how did you begin?**

I started at the BSI nearly ten years ago and have worked in various positions since then. I began working here in 2006 as a student writing my bachelor's dissertation at the BSI. I then got a permanent position as an administrator and was given civil servant status in that role in 2009. I went on to complete a master's degree and successfully applied for a specialist advisor post in 2011.

### **What is your job and what does it involve?**

I work in the Secure eID Applications unit, where I am mainly involved in developing and implementing eID infrastructures.

An example is smart metering Public Key Infrastructure (PKI), which enables secure transmission of data from networked electricity meters. Another area of my work focuses on using the online identification function of ID cards to derive electronic identities for specific applications. Essentially, I develop and assess technical concepts and standards, and manage projects which incorporate these in applications.

### **What first prompted you to apply to the BSI?**

I became interested in IT security early on and developed my interest through

my choice of lectures at university. While I was writing my bachelor's dissertation, I realised I really wanted to work at the BSI. I applied for a job as soon as I had finished my dissertation and was lucky enough to get a permanent position.

**How did you come to write your dissertation at the BSI and how exactly did you go about it?**

I first became aware of the BSI thanks to a colleague, Marcel Weinand, who has since retired. At the time, he was a lecturer in Common Criteria at Bonn-Rhein-Sieg University of Applied Sciences where I was studying. He offered me the opportunity to write my bachelor's dissertation at the BSI. Looking back, I am very glad he did. I worked in an office at the BSI where I was able to chat and exchange ideas with other colleagues. I experienced the day-to-day work and the working environment first hand, which not only helped me with my bachelor's dissertation, but also made it easier to decide what I wanted to do after graduation and where I wanted to work. By the way, the topic of my dissertation was the development of a security standard for USB devices. It is great to see that this standard is now actually being used in products.

**What opportunities for career advancement does the BSI offer a graduate with a bachelor's degree?**

Bachelor's and master's degrees are the foundation for different career paths in the upper and senior civil service. Further advancement usually happens within these career paths. Alongside my work, I completed a master's degree by distance learning, which then opened up the opportunity for me to apply for a specialist advisor post and switch to the senior civil service career path.

**What makes the BSI stand out as an employer? What is so special about working here, especially as opposed to a job in the private sector?**

What I like most about working at the BSI is that I am always dealing with current and very innovative topics. Working here has never been boring. I was very well accepted as a career entrant and was able to gain practical experience quickly. I can't compare it to the private sector because I've never worked there. Essentially, I see it as an advantage that here you can really focus on bringing forward all the different aspects involved in projects because economic success is not the main priority.

**Civil servants are generally not regarded as particularly innovative, are they?**

Being a civil servant is not so bad. A secure job is a wonderful thing and you can build on it in many different ways. Also, the BSI is not a traditional administrative authority but a technical service provider. There are lots of opportunities to take forward various projects. Over the years, I have worked on a number of major government initiatives including electronic passports and ID cards, and also smart metering. It is great when you know your work is highly relevant to everyday life and you can actually see the outcome of your efforts, such as the ID card in your wallet. ●

**The BSI as an employer**

The BSI currently employs around 600 people, most of whom have a higher education qualification in engineering, maths, computer science or physics. Teamwork and project work are strongly encouraged at the BSI in order to ensure we are able to respond to technical challenges in a flexible manner. It is our aim to always be one step ahead in the field of IT security. Therefore, the willingness of our employees to take advantage of our excellent training opportunities is a key requirement.

Find more information about working at the BSI, current vacancies and information on training, student support and dissertations at: [www.bsi.bund.de/jobs](http://www.bsi.bund.de/jobs).



---

## Legal Notices

---

Published by:	Federal Office for Information Security (BSI), 53175 Bonn
Source:	Federal Office for Information Security (BSI) Section B23 – Public and Press Relations, Godesberger Allee 185–189, 53175 Bonn, Germany Phone: +49 (0)228 999 5820; e-mail: <a href="mailto:oeffentlichkeitsarbeit@bsi.bund.de">oeffentlichkeitsarbeit@bsi.bund.de</a> ; internet: <a href="http://www.bsi.bund.de">www.bsi.bund.de</a>
Last updated:	March 2016
Content and editing:	Stephan Kohzer and Nora Basting, Federal Office for Information Security (BSI); Joachim Gutmann, GLC Glücksburg Consulting AG
Concept, editing and design:	Fink & Fuchs Public Relations AG (FFPR), Berliner Straße 164, 65205 Wiesbaden. Internet: <a href="http://www.ffpr.de">www.ffpr.de</a>
Printed by:	Druck- und Verlagshaus Zarbock GmbH & Co KG, Sontraer Str. 6, 63086 Frankfurt/Main, Germany. Internet: <a href="http://www.zarbock.de">www.zarbock.de</a>
Item number:	BSI-Mag 16/703-1e
Image credits:	Title: Fink & Fuchs Public Relations AG; p. 4: Jordan Tan/Shutterstock (top left), Ed Gregory/pexels.com (top right), Fink & Fuchs Public Relations AG (centre), Matej Kastelic/Shutterstock (bottom left), Fink & Fuchs Public Relations AG (bottom right); p. 8: Airbus Group press office; p. 9: Jordan Tan/Shutterstock; p. 10: Airbus Group press office; p. 13: Idealistock/iStock; pp. 16–17: Anne Hartwich; p. 19: Jesco Denzel/BPA; p. 20: Ed Gregory/pexels.com; p. 23: Bene Images/Shutterstock; p. 24: Federal Ministry of the Interior; p. 25: BMI; p. 26: Fink & Fuchs Public Relations AG; p. 30: Leo Leowald/BSI (top right); p. 30: BSI; p. 31: BSI; p. 34: Fink & Fuchs Public Relations AG; p. 36: Federal Ministry of Transport and Digital Infrastructure; p. 37: Ivan Smuk/Shutterstock; p. 38: Fink & Fuchs Public Relations AG; p. 40: Julia Tim/Shutterstock; p. 41: Anne Hartwich; p. 43: Matej Kastelic/Shutterstock; p. 44: Stephan Kohzer/BSI;

The BSI 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.



.....



For the digital version of the BSI Magazine, scan the QR code

