Federal Office
for Information Security

BSI Magazine 2017/01

Security in focus

Cyber Security Strategy for Germany 2016

BSI INTERNATIONAL

BSI: Key Role in the Avalanche Takedown

CYBER SECURITY

Ready for the New Level of Threat

THE BSI

180 New Minds for a Common Mission

EDITORIAL

A New Dimension

'The threat from professional and suspected state-sponsored cyber attacks is high'

Anchoring a message in the public mind is both a challenging and complex task. This is especially the case when something experts consider to be vital, but which the general public, business and public administration view as marginal, is concerned. The message of how important cyber security is has often gone unnoticed due to the latter view, which encouraged us to ignore the warnings regarding safety in the digital realms.

But times have changed. Since hospitals, power stations and telecommunications providers have been hacked and blackmailed, the Bundestag and political parties have become targets of attacks and the US intelligence services have reported interference in the US election by the Russian government, the issue of cyber security has now entered the consciousness of the public at large.

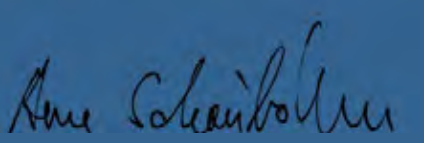
Important elections coming up soon throughout Europe, including in Germany. This is reason enough to be concerned about the targeted manipulation of public opinion by third parties, especially regarding campaigning in the 2017 Bundestag elections. Together with other European security authorities, the BSI is therefore attempting to prevent potential cyber attacks in the upcoming elections. The defence capabilities of governmental networks are continuously optimised.

The threat from professional and suspected state-sponsored cyber attacks is high. As can be read in our current status report, around 44,000 infected emails were found in government networks before they were able to reach recipients' inboxes. This represents a fourfold increase over the previous year. Around 20 highly professional attacks occur daily on government networks.

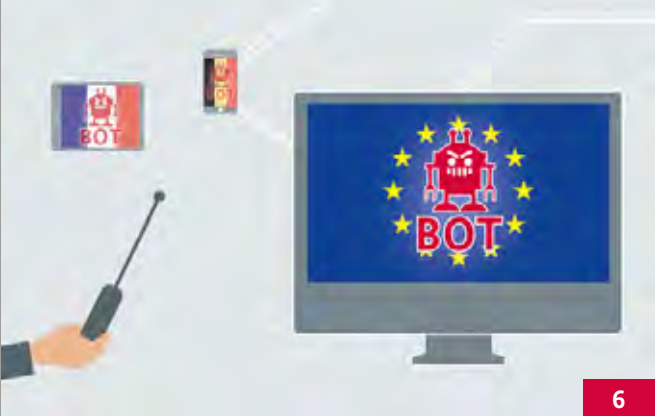
But it is not only the attack itself that represents a hazard – much worse are the political dimension and the effect of these attacks. The attacks do not even need to succeed. They need only sow doubt that the outcome of a democratic election, rather than being the result of the ballot box, has been decided by a team of hackers, state-sponsored or otherwise.

Therefore public awareness of the importance of cyber security cannot be stressed enough. We must take this opportunity to increase security. We need to keep providing information that is publicly effective, and we need to show how we are successfully enhancing Germany's capacity to repel any type of cyber threat. The BSI, as the national cyber security authority, is taking a decisive role in this.

I hope you find the articles stimulating.



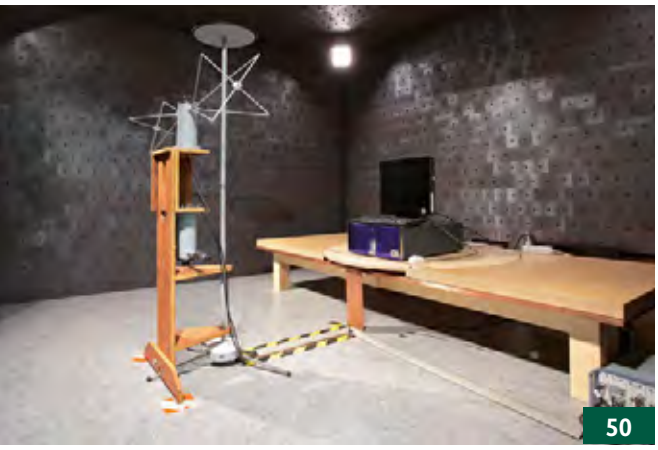
Arne Schönbohm
President of the Federal Office for Information Security



6


16


32


50

58

TABLE OF CONTENTS

NEWS

Photo: Catharina Frank

ECSM

European Cyber Security Month

In October 2017, the BSI once again participates in the European Cyber Security Month (ECSM, https://cybersecuritymonth.eu/). The European-wide month of campaigning is intended to raise IT security awareness among EU citizens, organisations and businesses and to focus attention on the risks to cyber security. Led by the European Union Agency for Network and Information Security (ENISA), initiatives, events and awareness campaigns are held throughout October. The BSI acts as a coordinating body for Germany, in addition to participating through its own activities.

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

Review

The sixth German Prize for IT-Security 2016

For the sixth time, the Horst Görtz foundation awarded its German IT Security Prize in Darmstadt in October. For the first time, the prize fell under the patronage of Prof. Dr Johanna Wanka, Federal Minister of Education and Research. From 45 submissions, a jury of experts selected the best innovations from the fields of IT security, cryptography, system and network security, and defence against cyber attacks. The Foundation hopes that these prizes will make a small contribution to 'Made in Germany' IT security. The jury is made up of IT security experts from business and academia.

Secure E-Mail Service

Posteo as first to receive Certification

In December 2016, BSI published the final version of the 'Secure E-Mail Transport' guidelines and the test specifications pertaining thereto, on the basis of which Posteo was the first e-mail service provider to be issued with a certificate for secure e-mail services. Posteo was able to successfully demonstrate conformity to the BSI's 'Secure E-Mail Transport' Technical Guideline, and therefore received the corresponding certificate from the certification agency Datenschutz cert. As Arne Schönbohm, BSI President, explained, 'Our Technical Guideline sets new standards for cyber security in digitalisation, from which both e-mail providers and users benefit in equal measure.'

https://www.bsi.bund.de/dok/8664710

CeBIT 2017

The BSI at CeBIT 2017

During 20–24 March 2017, the BSI will be at CeBIT focusing on issues of cyber security, IT-Grundschutz, and mobile security. Visitors can obtain further information at the BSI stand about offers and solutions for increased IT and cyber security for government, business and society. Graduates and job-seekers can also learn more about career opportunities within the cyber security agencies. The BSI stand can be found at CeBIT 2017 in Hall 6, Stand H30.

CSCG

Cyber Security Challenge Germany

There continues to be a demand for talented young personnel in the IT security sector. The Institute for Internet Security and the TeleTrusT IT Security Association Germany were searching for new talent at their annual 'Cyber Security Challenge Germany' (CSCG, https://www.cscg.de/). From May onwards, young hackers ages 14–30 will be called upon to solve interesting online challenges. The winners of the final in Berlin in September can then measure themselves against the European elite in the European Cyber Security Challenge (ECSC).

E-world energy & water

Review

The BSI exhibits at the E-world 2017 trade fair

For the fifth time, the BSI had a stand at the 'E-world energy & water' trade fair which took place in Essen during 7–9 February 2017. With more than 24,000 visitors and 640 exhibitors, E-world is the leading European fair for the energy and water sector. The BSI again provided information on security and interoperability requirements (protection profile, Technical Guideline TR-03109) for the smart meter gateway, the smart metering PKI and certification meeting common criteria, as well as information security in managing and operating intelligent measurement systems.

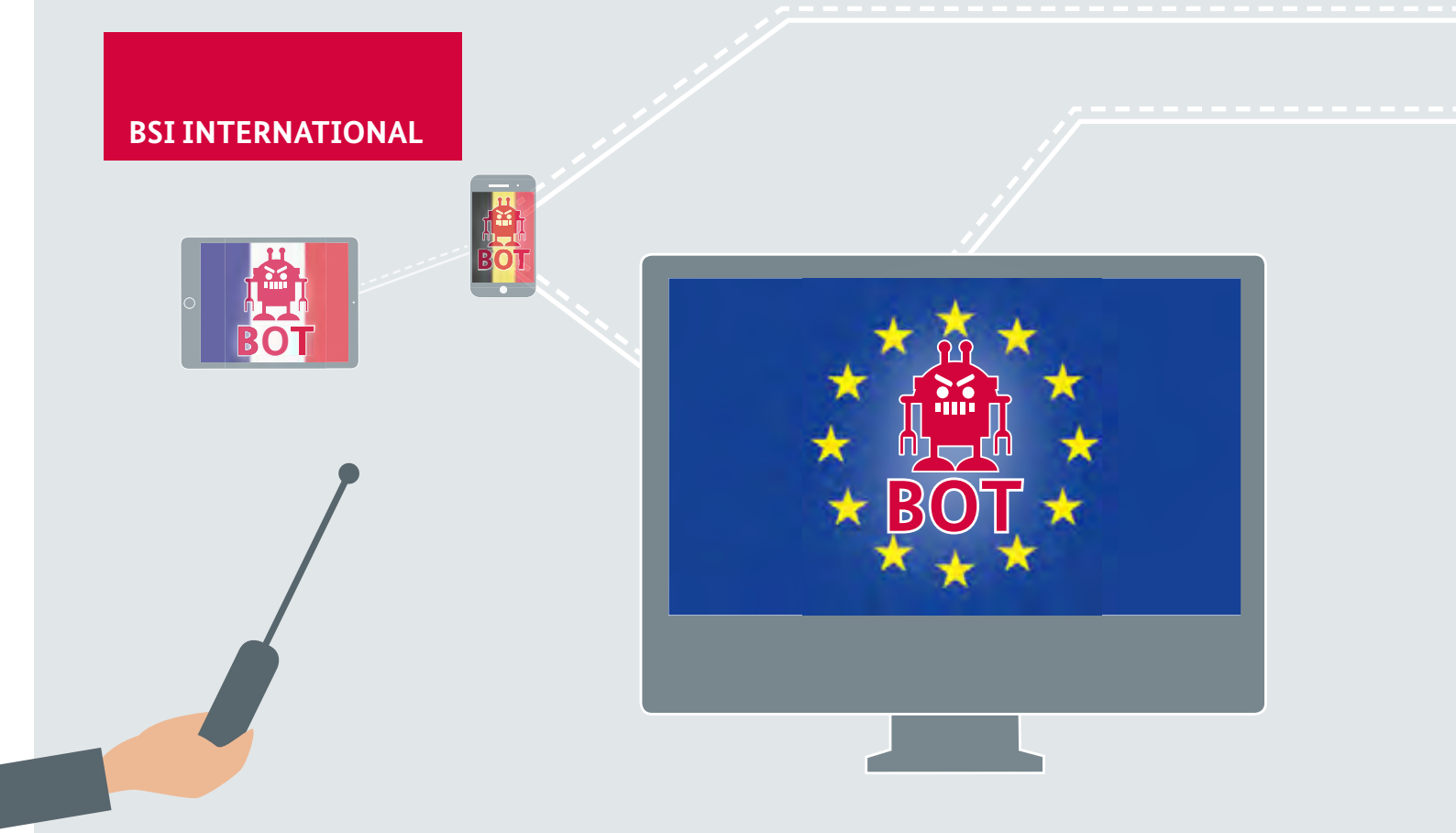
www.bsi.bund.de/SmartMeter

On the Home Straight

Modernising the IT-Grundschutz

Major progress has been made in revising the tried and tested BSI method for establishing an integrated information management system. A community draft, issued in the autumn of 2016 concerning the 200-3 risk management standard, included for the first time every risk-relevant step in implementing the IT-Grundschutz. Users can therefore in future achieve the required level of security with significantly less effort. The 200-2 standard on the IT-Grundschutz approach will be presented at CeBIT 2017. The issuing of these two publications means two milestones have been achieved in modernising the IT-Grundschutz. As a next step, further elements of the IT-Grundschutz compendium will be issued.

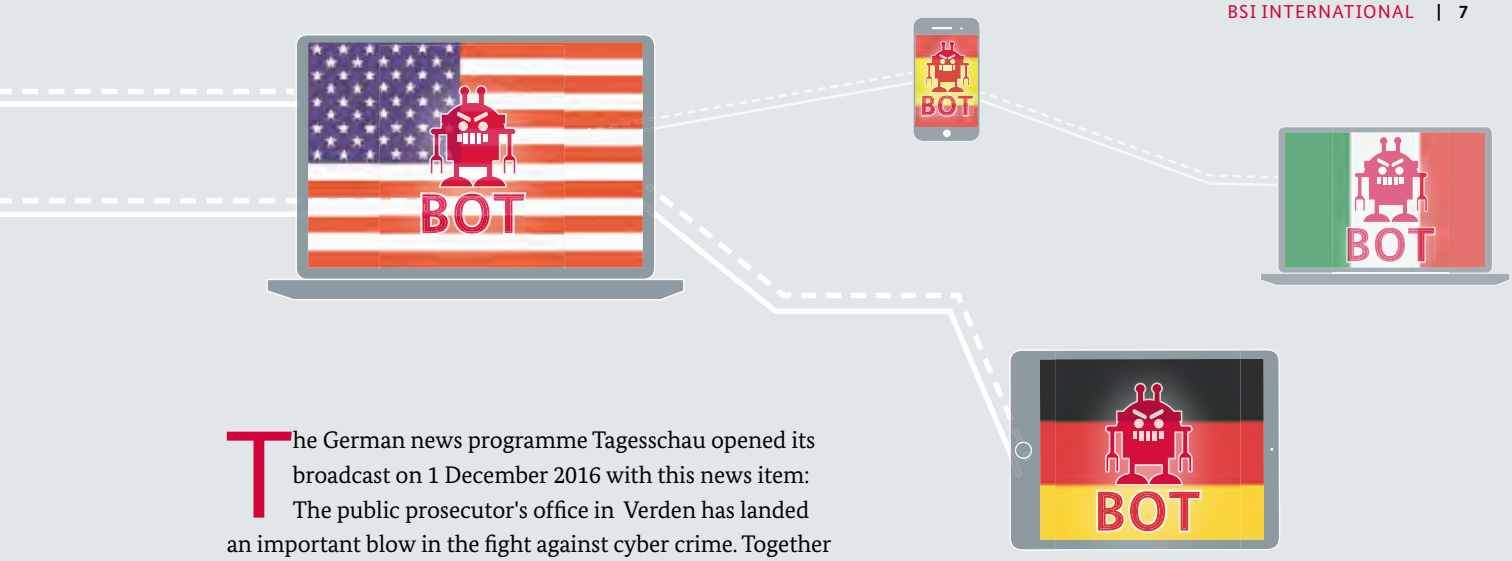
BSI INTERNATIONAL



BSI: Key Role in the Avalanche Takedown

A Blow to International Cyber Crime

On 30 November 2016, German law enforcement agencies struck a huge blow against international cyber crime. The taking down of the Avalanche botnet infrastructure removed a malware ring which has brought harm to millions of internet users worldwide since at least 2009. Looking more closely at an investigation that has been going on for years, it becomes clear that it is not by chance that those involved in the hunt are to be found at the heart of the federal republic. The BSI, as the national cyber security authority, made an internationally significant contribution to this key victory in the ongoing fight against internet crime. The 'Avalanche' is a prime example of the BSI's significance as a key player in information security for the government, business and society in the digital era, with respect to prevention, detection and response.



The German news programme Tagesschau opened its broadcast on 1 December 2016 with this news item: The public prosecutor's office in Verden has landed an important blow in the fight against cyber crime. Together with Lüneburg's central criminal investigations department (ZKI), those responsible for the Avalanche botnet, which has been operating since at least 2009, could be arrested. Federal Minister of the Interior Thomas de Maizière called the action unique and described it as 'a statement of intent in the fight against international crime in cyber space'.

The arrests represent a high point in an investigation that has been going on for years. The nature of internet crime means it cannot be resolved using traditional methods of criminal prosecution – simply because the Internet recognises no national borders. Authorities and institutions from more than 30 countries were involved in the preparations. These included law enforcement agencies from the USA, including the FBI, as well as Europol, the non-profit organisation 'The Shadowserver Foundation', Fraunhofer FKIE and other international partners. Close cooperation throughout the investigation via face-to-face meetings as well as telephone and video conferencing between all those involved, including the BSI, was of major importance for the case's success.

PROVIDING THE TECHNICAL EXPERTISE

In addition to the public prosecutor's office in Verden and the ZKI Lüneburg, a number of other institutions within the federal republic were involved, such as Lower Saxony's state criminal office (LKA) and the federal criminal office BKA. In the action against Avalanche, the BSI played a top role supported by botnet researchers from the Fraunhofer FKIE. Although the BSI is not a law enforcement agency, it was able to make a vital contribution in apprehending the perpetrators through its technical expertise and infrastructures.

Support for the law enforcement agencies included binary code analysis of malware from more than 20 botnets, analysis of C&C servers, the generation of botnet domains and the creation of innovative sinkhole mechanisms including the necessary software.

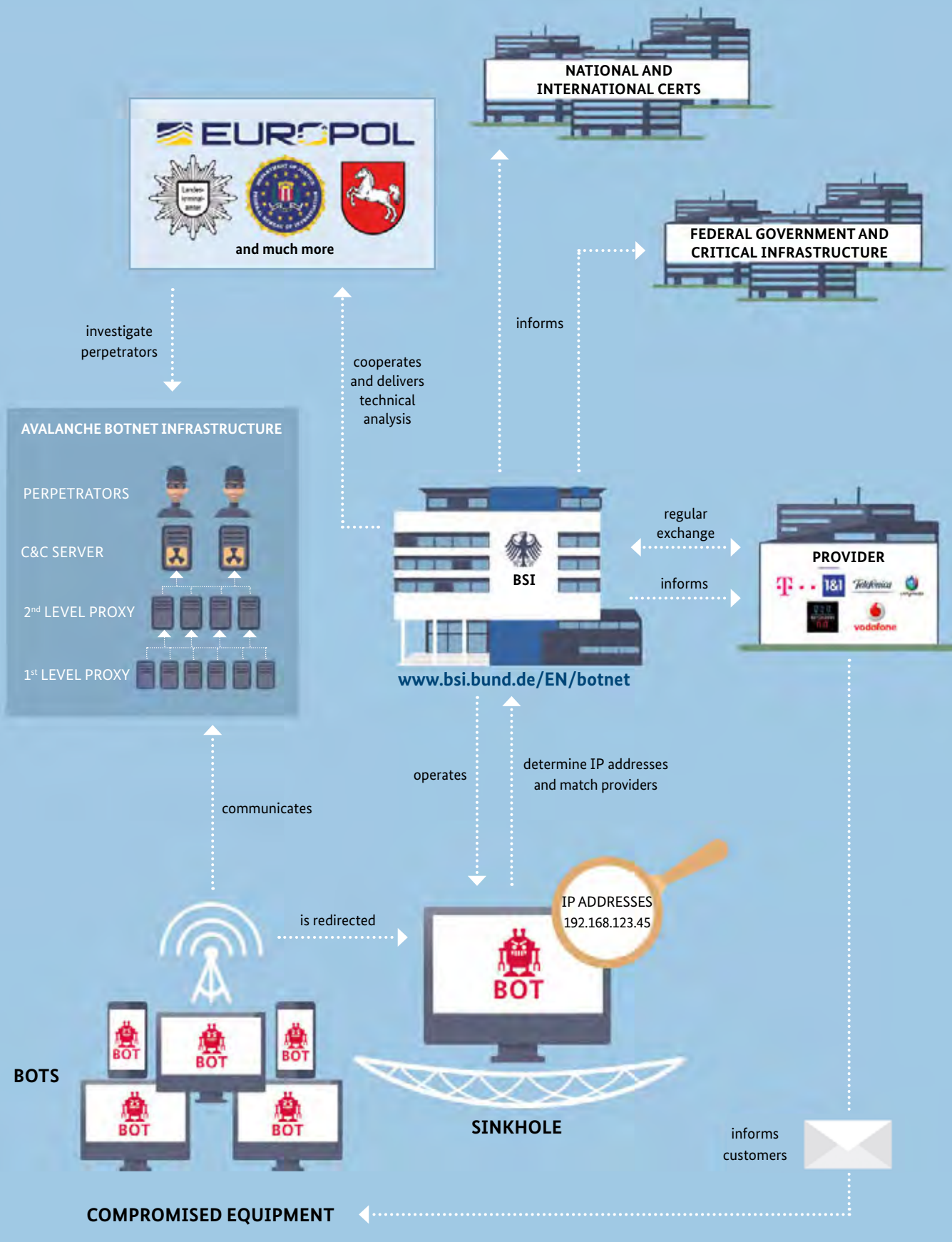
Avalanche is not the first botnet infrastructure to be successfully taken down. However, this case was special because not only were 20 botnets simultaneously disconnected, but the action also fully supported and involved law enforcement agencies right from the outset. Frequently, botnets blocked by IT and security companies soon reappear somewhere else because the originators are not prosecuted . Conversely, law enforcement agencies in other countries do not have the kind of technical support provided by BSI in the fight against cyber crime.

What got the ball rolling were the criminal charges brought by victims of a wave of attacks by ransomware known as the 'Windows Encryption Trojan' in 2012. These victims fell into the trap of the first noticeable Avalanche attacks by opening attachments to phishing mails concealing ransomware. This software then encrypted user hard drives and displayed a message demanding payment of a 'ransom' – otherwise the data would remain forever encrypted. Following initial investigations by the ZKI Lüneburg and the public prosecutor's office in Verden, a request for support was made to the BSI in the summer of 2013.

THE SHADOWSERVER FOUNDATION

The Shadowserver Foundation was established in 2004. This association of volunteer internet security specialists aims to make an active contribution to the fight against internet crime. A central element of their work is the gathering of information about infected systems and criminal structures, and forwarding this to warn those affected. The team of experts supported the Avalanche case as an interface to the domain registries as well as by providing servers to set up sinkholes. **For more information see www.shadowserver.org.**

TAKING DOWN THE AVALANCHE BOTNET INFRASTRUCTURE



PROTECTION OF CITIZENS THE TOP PRIORITY

Right from the early phases of the undercover investigations of the criminal prosecutors, the BSI's focus was on protecting internet users from Avalanche attacks. To achieve this, the BSI turned to an established infrastructure. There have been previous occasions when the BSI has issued warnings to citizens via its BSI für Bürger platform as well as working together with partners such as botfrei.de and the Anti-Botnet Advisory Center. A little later in January and April 2014, the BSI warned the public twice about the effects of a theft of 37 million identities. This crime was also down to the puppet masters behind Avalanche, despite no proof having emerged from the ongoing investigations.

Internet providers are flooded daily with reports about infected systems, some of which, however, are incorrect and contain inaccurate data. As a consequence, victims cannot be informed. To confront this problem, the BSI, together with the PI provider information system, established a unique global information channel. Infection reports from high-quality and approved BSI sources are then processed with high priority by the providers. Only providers, and not the BSI, can match IP addresses to network connections. The BSI believes that this was the start of an unprecedented global collaboration. Since August 2014, the BSI has been using this method to inform providers hourly about infected computers. The providers are able to use the IP addresses to trace which customers have been affected and to therefore warn them. Users could then be protected from the effects long before the takedown. The BSI also provides signatures, gleaned from analysing the investigated malicious code variants, to the producers of anti-virus software. Users of their software then benefit from this measure, providing they keep the software up-to-date.

THE TRAP CLOSES

In addition to protecting citizens, the BSI has further investigated and analysed the extent of the botnet infrastructure – an enormous task also because of Avalanche's extremely broad spread. It was later discovered that victims were located in more than 180 countries. The infrastructure was also highly complex. It was made up of multiple proxy servers to conceal the actual command and control server which was using double-fast-flux technology – this enabled server locations and domains to change instantly to avoid detection. Armed with this knowledge, the BSI was able to help prepare the final decisive step: the taking down of Avalanche on 30 November 2016 by seizing or blocking more than 800,000 domains. Five arrests followed with 37 house searches and the confiscation of 39 servers from different countries – a further 221 servers were shut down by the hosting providers.

The investigation is not yet at an end but the takedown is a major victory and has helped to make the Internet a more secure place. For at least one year, bots will be redirected to a sinkhole so that the botnets can no longer be used by criminals. This gives users time to clean their computers and better protect themselves. ■

SINKHOLING

A sinkhole is a computer system to which queries from botnet-infected systems are redirected. In the case of Avalanche, the BSI worked with the Fraunhofer FKIE and the Shadowserver Foundation to set up the sinkhole infrastructure. Bots from the Avalanche infrastructure were then unable to communicate with the originating server – their control over infected computers was therefore broken. To establish a sinkhole requires knowledge from the authorities about the botnet domains of the Avalanche botnets. This is the only way that domains can be redirected to the sinkhole server to prevent bots being controlled by perpetrators. Sinkholes provide a further benefit. The sinkhole system registers queries from requesting computers, along with IP addresses and access time. The BSI was therefore able to identify the users' providers and forward them the IP addresses. The providers were then able to use the IP addresses to identify affected customers, and issue warnings and recommendations on disinfecting their computers. Sinkholes are therefore essential infrastructure for taking down botnets.

For more information see https://www.bsi-fuer-buerger.de/EN/botnet

A new Label for Cloud Security

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

BSI and ANSSI Jointly Develop ESCloud Label

With the founding of the 'ESCloud' working group, BSI and ANSSI (Agence nationale de la sécurité des systèmes d'information) are jointly starting up a cloud security initiative. Put into perspective, this should feed into pan-European cooperation.

On 12 December 2016, Arne Schönbohm (President of the BSI) and Guillaume Poupard (Directeur général of the ANSSI) signed a Memorandum of Understanding, thereby establishing the 'ESCloud' Working Group which will develop the label further. The following day, this was presented publicly to an audience of dignitaries from politics and business at the digital conference as part of the German-French consultations. Federal Minister of the Interior Thomas de Maizière naturally insisted on personally underlining the importance of the project.

The project is consistent with the continued collaboration between the two national cyber security agencies, which has proved successful over many years.

NEW METHODS OF COOPERATION

The ESCloud Label and the Working Group represent an entirely new direction. Under the current cooperative arrangements (e.g. certification under common criteria) agreement was reached on a joint form of testing which is then implemented by partners in a similar way and to a similar quality standard. The other partners can therefore accept the outcome as their own.

ESCloud takes this a step further. Entirely different approaches are unified under the quality label; these are approaches which both define and verify the security of cloud services. The ANSSI has their own certification under 'SecNumCloud' and the BSI has the auditor's opinion based on the BSI Compliance Controls Catalogue (C5). Both arrive at a level of security which professional cloud services are expected to achieve in all cases.

This construct only functions because it is based on a range of existing requirements. To start with, it requires broad consensus on the objectives relating to the information security of cloud services. These are referred to as the Core Principles of the ESCloud. Confidence in the fact that the method adopted by the other party is of an equivalent quality standard is also required. This confidence increases based on positive experiences over many years. The decision to

From left to right: Directeur général of the French cyber security authority ANSSI Dr Guillaume Poupard, Federal Minister of the Interior Dr Thomas de Maizière and president of the BSI Arne Schönbohm

take one or the other approach is certainly well-justified in each case and is based on the assumption of certain conditions, which differ in Germany and France. Both methods achieve the objectives. Finally, competitive thinking or a negative 'not invented here' attitude must not be allowed to become a factor in this context, as this would then make a mockery of the joint work being conducted.

It is the many years of cooperation and the common goal which make it possible for the BSI and the ANSSI to follow this route.

EUROPE IN VIEW

With healthy self-confidence and proven expertise – inherent in both agencies – the group of those working on the ESCloud might be further expanded in order to give the entire project a more pan-European dimension. This would clearly emphasize European values such as collaboration and the trust between different nations and cultures; instead of attempting to harmonize everything, we strive towards a common goal and are not deterred by differences.

CONSTANT COMMUNICATION

BSI was again represented at the French IT Security trade fair 'Forum FIC' (Forum International de la Cybersécurité) and had the opportunity to present the BSI Compliance Controls Catalogue C5 and the ESCloud together with the ANSSI at a well-attended workshop during the trade fair. The new BSI Vice President, Dr Gerhard Schabhüser, took advantage of his time at the trade fair to develop contacts and to gain a better understanding of market participants. This helps to develop solutions in both countries to find the best way of addressing challenges across national boundaries. ■

ESCloud

For more information see https://www.bsi.bund.de/EN/ESCloudLabel

C5 – Practical Cloud Compliance

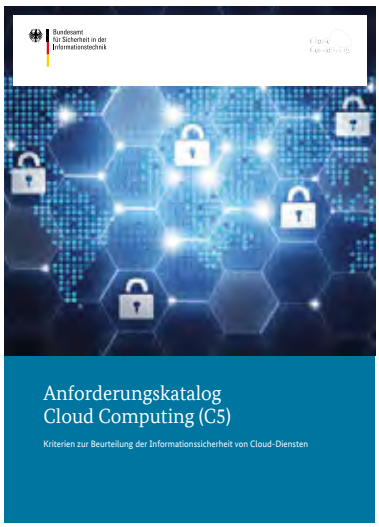
By Dr Markus Held, head of section Information Security in the Cloud and in Applications

Security Recommendations for Cloud Computing Providers

Cloud computing is an essential element in digitalisation. Business processes and business models are changing faster than ever before, both operationally and strategically. In order for value added processes to function sustainably, it remains necessary to ensure that the appropriate IT security is in place.

The Cloud Computing Compliance Controls Catalogue (C5) introduced by the BSI at CeBIT 2016 was so well received by the market that the first certificate based on the C5 has already been awarded to Amazon Web Services. C5 outlines the minimum cloud service security requirements which must be met at all times where the cloud is used in a professional context. This includes the transparency requirements regarding framework conditions for cloud provider service provision (e.g. system description, statements regarding the competent jurisdiction and government access rights to the data).

The BSI advises companies and authorities to insist that cloud providers are contractually required to comply with the C5 at least. Respective evidence should be a vital requirement. The fulfilment of the requirements and accuracy



From left to right: Board Spokesman for PwC Germany Dr Norbert Winkeljohann, Vice President of Compliance at Box, Inc. Crispen Maung and BSI President Arne Schönbohm at the presentation of the C5 certificate to Box

of transparency information must at least be verified by submission of a test report authenticated by auditors. On the one hand, cloud customers are able to make an informed decision on this basis, on whether a cloud service satisfies their own requirements, whilst on the other, the C5 concepts explicitly allow customers to negotiate their own higher level requirements with cloud services.

BSI IN DIALOGUE WITH BUSINESS REGARDING CLOUD COMPUTING

At the beginning of February 2017, the BSI invited representatives of industry and business-related authorities to 'The BSI in Dialogue' event on the issue of cloud security to Frankfurt am Main. In his welcoming address, Dr Norbert Winkeljohann, Board Spokesman for PwC Germany, underscored the need for the clear organisation of cloud computing security within digitalisation. BSI President Arne Schönbohm highlighted the strategic importance of cloud computing security for the BSI as the national cyber security authority. He also called for the security level defined in the compliance controls catalogue (C5) to be the minimum compliance level when the cloud is used in a professional context. He also announced the publication of a BSI minimum standard relating to secure cloud use and explained that this would encourage all federal authorities to demand C5 when using external cloud services. In his presentation, Dr Markus Held, head of Information Security in the Cloud and Applications at the BSI provided an overview of the BSI's cloud security portfolio, which is being continuously developed based on its results in practice. Prof. Dr Georg Borges, the well-known data protection expert from Saarland University, then explained the TCDP cloud data protection certification. Following on from this, Markus Vehlow – partner at PwC – explained how to implement common auditing of data protection and IT security of cloud services based on TCDP and C5 more efficiently. The cloud provider view was represented by Crispen Maung, Vice President of Compliance at Box, Inc. who stressed the point that security standards compliance was a key competitive factor for cloud providers. The culmination of the event was the presentation by PwC of the newly acquired C5 certificate to Box, Inc., represented by Crispen Maung.

CONCLUSION AND OUTLOOK

The minimum standard for secure use of cloud services will encourage federal government offices to implement appropriate processes to ensure cloud security, as well as to ensure compliance with the C5 when procuring cloud services. In addition to this, the BSI will soon publish a joint paper with the ISACA, the international association of IT auditors, which will support auditing of cloud providers or of cloud customers based on C5 by internal auditors.

The BSI places emphasis on practical relevance and on close dialogue with all stakeholders from government, business and society in the ongoing development of C5 and the associated product portfolio. The BSI will consistently and continuously maintain and further develop its cloud security standards on this basis. ■

At the end of January, the German cabinet passed the draft legislation for the implementation of the EU guideline on Network and Information Security (NIS guideline). The NIS guideline, which entered into force in August 2016, defines measures for ensuring a high level of common security for network and information security systems in the European Union. This created a standard legal framework for the EU-wide development of national capacities for cyber security and a basis for stronger collaboration between member states of the European Union, as well as minimum requirements and reporting obligations for specific services such as cloud services and online marketplaces. In light of this, the BSI has been given new responsibilities and powers – this is a key requirement for the continued improvement of cyber security in Germany.

Draught Legislation on the NIS Guideline:

Increased Responsibility and Powers for the BSI

Implementation Required by May 2018

The NIS guideline is an important step towards greater cyber security in Europe. The Federal Government has now also established the basis for implementing European standards in national legislation in a prompt and timely manner. This began from a very good starting point: A standardised legal framework governing collaboration of government and business for the purpose of greater cyber security in critical infrastructures (KRITIS) has already been in place in Germany since July 2015 in the form of the IT Security Act. It requires KRITIS operators to implement a standard of IT security in accordance with state-of-the-art security measures and to report significant security incidents to the BSI. The draft legislation regarding implementation of the NIS guideline now extends the BSI's supervisory and enforcement powers relating to KRITIS operators. At the same time, it also strengthens collaboration between the federal states and the BSI. For example, in the future, the BSI will now be able to provide even more comprehensive support to the federal states, and to make the BSI's technical expertise available to them.

INCREASED POWERS FOR THE BSI

Despite the increased powers, the BSI will seek to ensure that the co-operative approach enshrined in the IT Security Act continues to be followed when implementing the NIS guideline, as challenges can only be addressed jointly by government and business. The BSI is therefore justifying its lead role in Europe in the area of cyber security. At the same time, the draft legislation is a useful addition to the IT Security Act. This is because, in future, providers of digital services will also be subject to minimum requirements and reporting obligations. Both online marketplaces and search engines as well as providers of cloud computing services are affected by this. The Federal Ministry of the Interior anticipates that between 500 and 1,500 companies in Germany will be affected by the new regulation. In its role as supervisory authority, the BSI will check compliance with the new requirements in future.

'The new NIS guideline is an important step towards greater cyber security in Germany. This is because the draft legislation represents the next step under the IT Security Act for ensuring a greater level of protection from cyber attacks for the government, business and the general public,' commented Arne Schönbohm, President of the BSI. 'The draft legislation must be implemented in national law by May 2018.'

HOW THE BSI SUPPORTS COMPANIES

Critical infrastructures linked to the Internet are a target for cyber attacks. It is quite possible that outages as a result of attacks may well, by themselves, result in losses running into the millions. In order to offer better support to those companies more effectively in the future, the BSI is currently setting up Mobile Incident Response Teams (MIRTs). This specialist task force is made up of cyber security experts from the BSI who examine particularly serious cyber attacks at the request of the operators on site and help to overcome them. An example would be a cyber attack which cripples key IT services. However, this would also include attacks on chemical facilities, as a result of which major risks to the population must be expected could justify the use of a MIRT, too. ■

CYBER SECURITY

WELL PREPARED FOR THE NEW LEVEL OF THREAT

German Cyber Security Strategy 2016

The Federal Government adopted the Cyber Security Strategy for Germany 2016 submitted by the Federal Minister of the Interior in November 2016. This forms the inter-departmental strategic framework for Federal Government activities relating to cyber security, and updates the cyber security strategy from 2011.

Five years is a very long time in the age of digitalisation. This period has been characterized by new possibilities in the area of communication and interaction, for example as a result of social networks, new areas of business such as the Internet of Things, and new fields of research and development such as self-learning machines. People's everyday working and home lives are increasingly being governed by networked electronic devices. Huge quantities of data are being created as a result of the rise in the automatic generation of data, and the increasing prevalence of smart detectors.

The threats to digital society as a result of cyber attacks have also changed over this period. Attackers have discovered new business models and are implementing these with increasing speed, for example in the area of extortion with the help of ransomware. New versions of ransomware which encrypt data and seek to extort ransom money are entering the market on a daily basis. The networking of devices in the Internet of Things such as smart TVs, network cameras or baby monitors has led to the creation of powerful botnets which are used for DDoS attacks with bandwidths which up to now have only been possible in theory.

Constantly changing circumstances also mean that responses need to be updated and expanded, and combined within a new cross-departmental strategy. The strategic approaches and aims of the 2011 cyber security strategy still largely apply today. Many of the measures planned in the 2011 strategy have now been implemented. As an organisational measure, the cyber security council, a high-level body for providing strategic impetus at the interface of policy-making and business, was created together with the Cyber Response Centre, which is a platform for strategic and operational exchange between authorities and is located at the BSI.

FOUR AREAS OF ACTIVITY

THE PRIORITIES FOR CYBER SECURITY POLICY OVER THE COMING YEARS FOCUS ON THE FOLLOWING FOUR AREAS OF ACTIVITY.

- Secure and self-defined action in a digitalised environment will be strengthened: This involves enabling all users to understand and assess the opportunities and risks when using information technology and to base their actions on this. Appropriate, reliable technologies and framework conditions must be in place and must be continually developed for this purpose. The intention is therefore to introduce a basic certification procedure for secure IT consumer products, the criteria for which will be determined by the BSI. In parallel with this, there will be a strengthening of existing resources in the BSI used for the development of technical guidelines, for certification and for the support of national accreditation bodies in the area of IT security.

- The aim is also to expand cooperation between government and business in cyber security. Reliable collaboration and close communication between government and business are vital for being able to ensure a permanently high level of cyber security in Germany. To achieve this, new approaches must also be taken in order to combine and benefit from the relevant expertise. Collaboration with providers plays a key role here. This applies in particular, in light of current attacks, to providers' measures for identifying cyber threats, for dealing with recognised incidents/infections, and for lessening the impact of ongoing attacks.

- An effective and sustainable national cyber security architecture will be established: It will aim to effectively integrate the different stakeholders at federal level and, in addition, to ensure that the federal states, municipalities and businesses are considered. The National Cyber Response Centre already provides the relevant structure at federal level, within which the individual stakeholders collaborate within the scope of their responsibilities. In future, this collaboration must be intensified and federal state involvement increased.

- Germany is very active in shaping European and international cyber security policy. In view of the transnational networking taking place in a digitalised world, a high level of cyber security can only be achieved by embedding and strengthening national measures in the relevant European, regional and international processes. Germany will continue to actively contribute to European and international cyber security policy-making, and in particular will be proactive in driving forward EU pilot projects which address legal and technical questions related to cross-border processing and use of data.

The Cyber Security Strategy for Germany 2016 provides more than 30 strategic goals and measures for the improvement of cyber security in these four areas of activity. The cyber budgets required for this will be determined by the department responsible in each case, i.e. the Federal Ministry of the Interior, the Federal Ministry for Economic Affairs and the Federal Ministry of Defence.

The guiding principle of the Cyber Security Strategy for Germany 2016 which has now been adopted is to guarantee Germany's sovereignty and capacity to act in the digital age. Its goal is to make it possible for Germany to best utilize the huge opportunities and potential of digitalisation. However, an essential requirement for this is that the security risks can be managed. The objective of the cyber security strategy is therefore to establish cyber security, to the extent that it is appropriate to the relevance of the networked information infrastructures and the level of protection they require, without limiting the opportunities and benefits of cyber space.

RAPID MOBILE RESPONSE TO ATTACKS.

Particular importance is attached to rapid assistance on site. This is because cyber attacks in recent times have shown that, over and above the usual IT security measures, barely any institutionalized government structures exist that are able to quickly assist those affected locally with the processing of an incident or in defending against an ongoing attack. This involves, on the one hand, tackling security incidents from a technical perspective and, on the other, the activities of the security agencies at a local level based on the statutory provisions in each case.

The goal is to close this gap in support services quickly in all government institutions involved with cyber response, and to do this using a form of mobile strike force. The coordination required for such deployment by the different authorities will take place in the National Cyber Response Centre, subject to legal contraints.

- Mobile Incident Response Teams (MIRTs) will be set up in the BSI. The plan is for these teams to analyse and clean up cyber incidents in organisations which are of particular relevance to the community. The MIRTs in the BSI, which will be operational in 2017, will be able to provide rapid assistance on site in tackling the technical aspects of security incidents at the request and with the consent of constitutional bodies, federal authorities and operators of critical infrastructures and in addition to key organisations, in cases where these incidents specifically involve the public interest. This would make it possible to monitor and mitigate against an attack in a more efficient manner, such as the attack on the German Bundestag in 2015. This support will aim to quickly restore the security of the affected organisation's technical operations.

- A special investigation unit is to be set up in the Federal Criminal Police Office (BKA) to implement the first non-deferrable criminal procedural measures for the prosecution authorities, in consultation with the competent public prosecutor's office or the federal prosecutor's office. This comprises, in each case, four cyber crime experts from the BKA's existing and rotating 24/7 on-call service in order to implement immediate police measures required outside regular working hours.

- Mobile Cyber Teams will be established in the Federal Office for the Protection of the Constitution (BfV). These consist of IT specialists, intelligence experts with experience in evaluating cyber attacks and - where required - colleagues with foreign language skills. These cyber teams will be deployed in the case of a cyber attack with intelligence, extremist or terrorist origins. This also concerns potential sabotage attacks. The German Intelligence Service (BND) is able to monitor an attack both during the preparation and in the implementation phase.

- Military Counter-Intelligence (MAD) takes on this role in the area of defence. The flow of information resulting from the attacks is also registered. The German Armed Forces are able to use their organisational elements (including incident response teams) to contribute towards ensuring security at a national level.

STRATEGIC SUPPORT

A forward-looking cyber security strategy must not limit itself solely to defining strategic measures. The dynamic nature of digitalisation can only be managed by means of an ongoing strategy process, relating to issues of cyber security from which further strategic measures can be developed. New risks must be identified at an early stage and innovative solutions explored and developed. A key role in this will be assigned to the national cyber security council, which was established under the 2011 Cyber Security Strategy and acts as a strategic advisor to the Federal Government. Its role is being expanded, with the goal that the council will identify areas where action needs to be taken over the long term, as well as long-term trends, and use this knowledge to provide the platform to strengthen cyber security in the four areas of activity. In doing so, the national cyber security authority will also, in future, increasingly draw on expertise from society, business and science. ■

Three Questions for Federal Minister of the Interior Dr Thomas de Maizière

Why did the 2011 cyber security strategy need to be updated?

The strategic approaches and aims of the 2011 Cyber Security Strategy still largely apply today. However, in view of technical developments and the growing importance of digitalisation globally over the last 5 years, it was necessary to update the strategy last year. It forms the overall structure for all Federal Government activities relating to the improvement of cyber security in Germany. We are also seeking here to maintain the balance between freedom and security in the digital world.

Is the strategy already able to provide responses to the changing intentions of cyber attacks?

I assume that 'new intentions' refers to cyber attacks which are carried out seeking to influence the freedom we have to form opinions. These types of attacks might also precede attacks on the information technology of government, parliament or media companies. They may constitute a long-term threat to free society and democracy. Awareness, disclosure and clarification are needed here.

What is the role of the Federal Ministry of the Interior in implementing the strategy?

The Federal Ministry of the Interior coordinates the implementation of the cyber security strategy. State Secretary Klaus Vitt is responsible for this as Federal Government Commissioner for Information Technology. He is also chairman of the National Cyber Security Authority. The Cyber Security Council plays a key role in the implementation. The goal here is to identify areas where action needs to be taken over the long term, as well as trends, and to use this to provide impetus for strengthening cyber security. This strengthens the role of the cyber security council as strategic advisor to the Federal Government. The BSI is our key authority in all issues relating to cyber security.

For more information see https://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyber-Sicherheitsstrategie/cyber-sicherheitsstrategie_node.htlm

RELIABLE COLLABORATION

Five Years of Allianz für Cyber-Sicherheit

Cyber attacks can only be successfully prevented by means of close collaboration and ongoing communication in the response to risks. However, this requires the trust of all those involved. The Alliance shows how this can work in practice.

The Allianz für Cyber-Sicherheit was established as an initiative of the Federal Office for Information Security (BSI) and the Federal Association of Information Technology, Telecommunications and New Media – BITKOM. They searched for a method by which to interest and engage as many companies and institutions as possible, on a voluntary basis, in an issue which, entirely unjustifiably, has fallen off the radar: the joint cyber response. Established in 2012, 2045 institutions now belong to the Alliance, of which 101 are partner companies and 45 are disseminators.

As an association of all key stakeholders in the area of cyber security in Germany, the aims of the Alliance were to strengthen Germany's resilience against cyber attacks, to develop IT security expertise in German organisations, to provide current and valid information regarding threats in cyber space and to press ahead with the creation of a standardised assessment of the state of IT security. The initiative also supports the exchange of information and lessons learned between participants. BSI President Arne Schönbohm feels certain that 'the story of the Alliance is one of success, and is a great example of how IT security in Germany can be organised and implemented successfully.'

The basis of this is trust: As a platform, the Alliance provides a broad range of information on a wide variety of cyber security issues to companies, authorities, research and science as well as to other institutions. Monthly

status reports, warning notifications and ongoing background information provide registered Alliance participants with access to an extensive range of information, in particular related to the cyber security situation. Due to the partly confidential nature of this information, the distribution of this content must be strictly controlled and is subject to restrictions under the traffic light protocol (TLP).

Trust promotes the open sharing of experiences. Selected security themes are dealt with in regular workshops or training sessions for participants in experience groups (ERFA) within the Alliance. Expert groups of security specialists from business, research and the authorities discuss problems and propose solutions which then benefit participants. Partners and disseminators exchange information on partner days during CeBIT and it-sa, the IT security trade fair. Cyber security days in which non-members are able to participate take place quarterly. BSI President Arne Schönbohm is pleased that, 'the Alliance is ensuring the issue of cyber security is brought to a wider audience by each participant being able to benefit from the knowledge and experience of the other.'

This is because communication breeds knowledge: the Alliance's knowledge database. Its central components are the monthly report on the IT security situation and various items of thematic situation information. They are available to members of the Alliance. Depending on the topic, information is provided in the public, non-public or confidential areas. The database also contains various topic-related documents such as studies, surveys, tutorials, guidelines, warnings and a media library.

The Alliance has also contributed to developing trust in another form. The reporting area within the Alliance's Internet portal has proved to be an important source for integrating findings from cyber attacks into the BSI's overview of the current situation. Victims of attacks can report incidents in their organisations here. The report is made via an online form and may also be completed anonymously if necessary. The reports are evaluated statistically and technically, and are used in the preparation of the current overview of the IT security situation. 'To a certain extent, this has proved to be a blueprint for insights which might be gained from the reporting obligation under the IT Security Act,' believes Schönbohm. This is because cyber security is all the more strong if the response strategy is not only influenced by the BSI's knowledge but also by the expertise of as many other institutions as possible, and if the content is based on many different experiences.

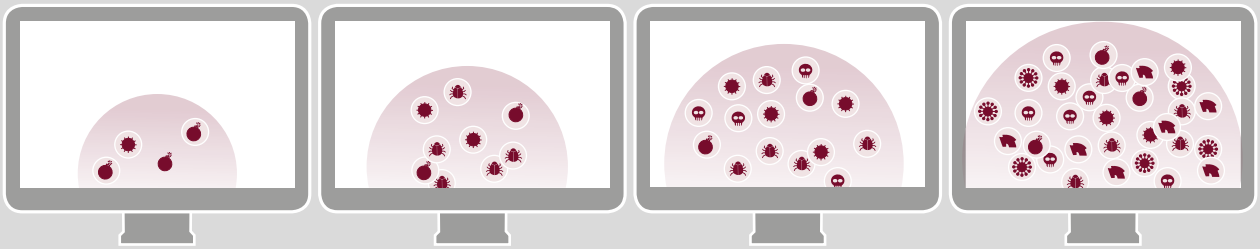
However, the intensive and open cooperation and communication in the Alliance also shows that Germany has chosen the correct route in organising the cyber response. BSI President Arne Schönbohm believes that 'the requirements for reliable collaboration were met in the first place by the fact that preventative and intelligence work was not completed in one and the same authority.' The success of the Alliance over the last 5 years shows that he is right. ■

Allianz für Cyber-Sicherheit

For more information see https://www.allianz-fuer-cybersicherheit.de

Digitalisation and Networking threaten IT Security

ANNUAL RISE IN KNOWN MALWARE VERSIONS

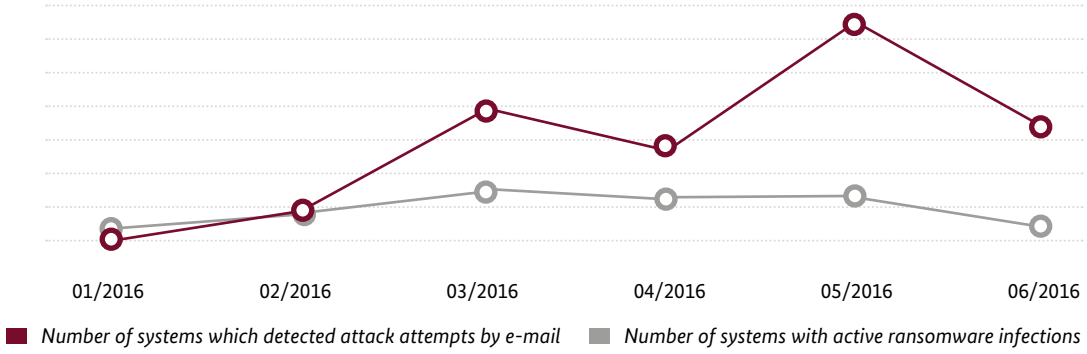


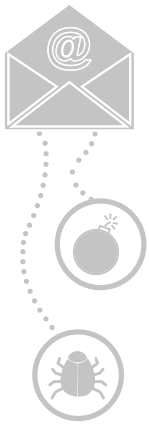
182.9 Mio.	326.0 Mio.	470.0 Mio	597.5 Mio
2013	2014	2015	2016

Source: AV-Test

RANSOMWARE ATTACKS: INCREASE SINCE 2016

Users should continue to be alert to unfamiliar and dubious emails.





INCREASE IN SPAM MAILS WITH MALWARE ATTACHMENTS

In the first half of 2016, overall spam activity increased by **73%** compared to the previous year. In the area of traditional spam however the increase was only **16%**.

By contrast, there was a massive increase in malicious software spread via spam mails of **1,270%**.

Increasing numbers of variants spread within a short space of time and, as a result, traditional responses cease to be effective. In 2016, around

380,000

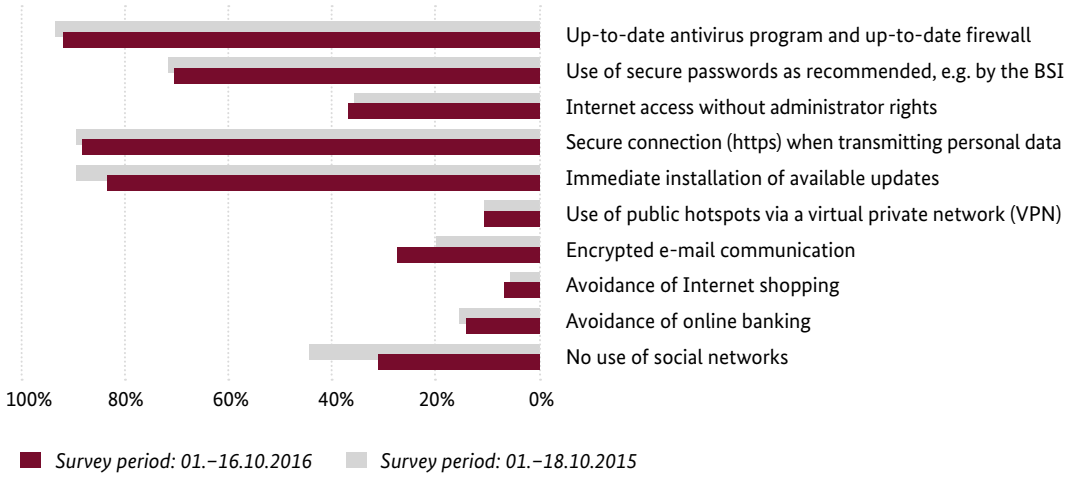
malware variants were detected on a daily basis.

For more information see https://www.bsi.bund.de/EN/SecuritySituation

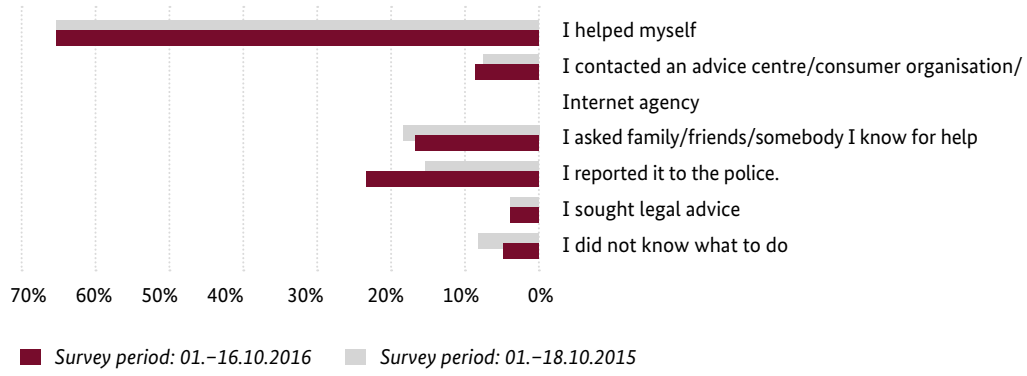
Source: Report on the State of IT Security in Germany (BSI)

Expertise in Managing Cyber Crime is on the Increase

AS LITTLE EXPENSE AS POSSIBLE: USERS RESORT TO ESTABLISHED PROTECTION MEASURES[1)]



VICTIMS OF CYBER CRIME TEND TO REPORT OFFENCES TO THE POLICE[1)]



IN SUSPICIOUS SITUATIONS, INTERNET USERS RESPOND BY ...[2)]

... leaving the website concerned or deleting the e-mail **(83.4%)**
... contacting the website operator **(12.9%)**
... contacting the Internet complaints office **(8.5%)**
... contacting the police **(26.9%)**

Only **3.1%** of Internet users do not respond at all in suspicious situations.

[1)] *Source for 2015: https://www.bsi.bund.de/dok/7023566, Source for 2016: https://www.bsi.bund.de/dok/8558402*
[2)] *Source: BSI/ProPK, Online survey 2015 and 2016 for the European Cyber Security Month (ECSM).*

Optimisation by Sharing

The DSCO – a Centre of Expertise for Cyber Security

Profile in brief:

Martin Wülfert has been head of the Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) based in Berlin since May 2016. He has master's degrees in Physics and Business Administration and is responsible for business development of the organisation which was established in November 2015. This includes, amongst other things, development of the portfolio, marketing and recruitment of members onto the Advisory Board.

The DCSO (Deutsche Cyber-Sicherheitsorganisation GmbH) is a cyber security competence centre and service provider for major enterprises in the German economy. The organisation was founded at the end of 2015 by the companies Allianz SE, BASF SE, Bayer AG and Volkswagen as a manufacturer-independent managed service provider.

The DSCO supports companies in protecting themselves and their supply chains from criminal hackers, industrial espionage, foreign intelligence services and sabotage - and in doing so, enhances Germany as a place to do business in the networked global economy.

Today, attackers are highly professional in the way they work and are extremely well organised throughout the kill chain. By contrast, there is often only limited or no cooperation at all among companies. Attackers simply have to identify a vulnerability, while businesses are forced to protect themselves against all potential attack vectors. This means that targeted attacks remain undetected for weeks, months or even years. This strong imbalance results in strategic disadvantages for business.

The DCSO adheres to the principle of 'optimisation by sharing': Operational knowledge of cyber threats and how to combat these is fed back to the DSCO and then automatically distributed anonymously to all other participants. This self-reinforcing feedback leads to greater security for all companies.

With the aid of a joint threat intelligence platform and internal network sensor technology, the DSCO helps its customers to detect attacks much more quickly. Together with the companies affected, a team of incident response experts develop effective strategies against attacks which have occurred. The DSCO also strengthens companies' ability to resist attacks by means of a technology evaluation service and a GRC platform (Governance, Risk Management and Compliance) which supports the security check of the supply chain.

As a company funded by German corporations, the DSCO operates entirely independently of manufacturers and is answerable solely to its members and customers. The focus of the DSCO is determined by an advisory board on which major customers, research institutes and authorities are represented. All profits made are reinvested in research and development.

The Federal Ministry of the Interior and the Federal Office for Information Security are key partners in the German economy. They have therefore been involved in the DSCO's competence centre and information exchange from the very start. ■

For more information see https://dcso.de/en

The IT Security Act

ACT ON INCREASING THE SECURITY OF INFORMATION TECHNOLOGY SYSTEMS (IT-SIG)

- Entered into force on 25 July 2015
- Requires operators of critical infrastructure to secure the information technology of their critical facilities using state-of-the-art security measures
- Obligation to provide evidence of IT security every two years
- Significant IT disruptions must be reported to the BSI

WHAT IS CRITICAL INFRASTRUCTURE?

- Organisations and institutions providing basic utilities (e.g. power, drinking water, food)
- Organisations where failure or impairment of their capacity to supply would result in dramatic consequences for government, business, and society in Germany

PART 1 OF BSI-KritisV IN FORCE SINCE 3 MAY 2016

- Sectors affected: Energy, information exchange and telecommunication, water and food
- A point of contact must be designated at the BSI no later than six months after entry into force of the regulation, and significant IT disruptions must be reported to the BSI (by 3rd November 2016)
- Two years available following entry into force of the regulation to implement state-of-the-art IT security and to demonstrate proof of this to the BSI (by 3 May 2018)

AMENDMENT TO THE REGULATION FROM SPRING 2017

- Sectors affected: Finance, insurance,transport and traffic and health
- A point of contact must be designated at the BSI no later than six months after entry into force of the regulation, and significant IT disruptions must be reported to the BSI (by autumn 2017)
- Two years available following entry into force of the regulation to implement state-of-the-art IT security and to demonstrate proof of this to the BSI (by spring 2019)

Federal Office for Information Security

THE BSI ...

- Evaluates and analyses reports received
- Related these to other reports and findings
- Uses this to prepare an overview of the current situation
- Sends warning notifications and alerts including recommendations for action to the critical infrastructure operators

POSITIVE RESULTS

- Over **85 %** of expected operators have designated a point of contact at the BSI and are being supplied with current information regarding the IT security situation
- **50 %** of energy suppliers and telecommunications providers have registered voluntarily
- Since 2007, the number of partners has grown from 40 to more than **430 organisations.**

UP KRITIS PROFILE & AIMS

- Public-private partnership
- Operators of critical infrastructure, associations and competent authorities
- Increase the resilience of critical infrastructure
- Ensure reliability of supply without restrictions wherever possible
- Implementation of the IT Security Act

UP KRITIS is a public-private partnership between operators of critical infrastructures (KRITIS), their associations and the competent authorities.

THE BSI

Introducing the New BSI Vice President

Interview with Dr Gerhard Schabhüser

Dr Schabhüser, you have recently taken up the post of Vice President. Where do you come from and what have you done in your career so far?

I am a native Westphalian and was born in Münsterland in 1961. I completed my degree with a master's in mathematics and was then awarded a doctorate in this field. My first professional position was with the BSI, which was established in the same year, 1991, and arose from the Central office for Information Security (ZSI).

At the BSI, I was initially responsible for the assessment of cryptographic methods. After a few years I moved over to design and therefore into developing encryption methods. Over this period I supported a large number of BSI projects relating to the provision of cryptographic systems in the field of classified information. After about 10 years, I became head of development of cryptographic methods. I then became head of the specialist field for cryptography and scientific basis as well as head of the department responsible for cryptography, scientific coordination and technical classified information security. I have now been Vice President of BSI since the start of this year.

What are your responsibilities as Vice President?

The priorities for my new office can be divided into three areas. The first describes my responsibilities for internal BSI policy. This area includes implementation of internal strategy, organisation of processes and adaptation of BSI structures to the increased size and to the profile requirements generated externally.

The second area is my role as advisor to the President. Here, I support the president in the positioning of the BSI, strategy development, evaluation of technology as well as reconciling political targets with technical implementation options.

The third area is sharing the burden involved in managing our public image. This includes representing the president at external engagements and presenting the BSI.

Which issues are the main focus here?

There is much to do in all three areas of responsibility. In the area of internal policy the focus is on the BSI's strong growth. For 2017 we have received approval for approximately 180 additional positions and as a result of this will grow to more than 800 employees. Our new colleagues must be recruited, trained and integrated. Internal processes and working methods must also be adapted as we grow. This is accompanied by a significant increase in work and, at the same time, a reduction in response times due to the increasing level of threat.

The other two areas tend to involve more ongoing processes resulting from day-to-day business.

What aims are you pursuing?

We want to make BSI fit to address the new challenges we face. This includes, for instance, adapting products and services to the increasing size of the BSI as well as the additional tasks and target groups. We were originally responsible for IT security in the state sector and primarily for federal administration.

'Increasing digitalisation requires ever stronger preventive IT security.'

Profile in brief:

Dr Gerhard Schabhüser has been the new vice president of the BSI since 1st January 2017. He succeeded Andreas Könen, who is now Head of IT and Cyber Security, Safe Information Technology at the Federal Ministry of the Interior. Schabhüser, who graduated in mathematics, has been involved in the BSI since it was founded in 1991. We spoke with him about his background, his experience and his responsibilities and goals in his new position.

Our scope here is also expanding due to the increasing use of IT technologies in more and more processes.

We are now also responsible for configuring the security of critical infrastructures, involving a much greater number of customers from new sectors. In the future, we will also address issues more closely on a state and municipal level, meaning we will require a significantly higher degree of scaling for our services and products in order to protect information – including prevention and reaction. Even though the BSI is growing, we will certainly not be able to do everything ourselves. We therefore need multipliers such as service providers and manufacturers, which we will qualify and commission accordingly so that we can offer solutions to the government, business and society.

What trends do you expect in the future?

Increasing digitalisation calls for ever stronger, preventative IT security. In light of this, at the BSI, we intend to respond quickly and flexibly to any sudden new requirements. In terms of the state sector, this may include protecting the IT systems used in elections. This year in particular, we may face new challenges as a result of the Bundestag elections.

For the economy target group, the focus of IT security legislation also primarily lies in the Internet of Things and Industry 4.0. In the future, further developments such as autonomous driving in networked cars or major digitalisation projects in cities will play a key role for us.

We also want to address and shape IT security as a key criteria for society. We are therefore substantially expanding our range of information services for citizens and our dialogue with civil society organizations. ■

ACTIVELY SHAPING CYBER SECURITY

THE BSI AS A PARTNER FOR THE ECONOMY

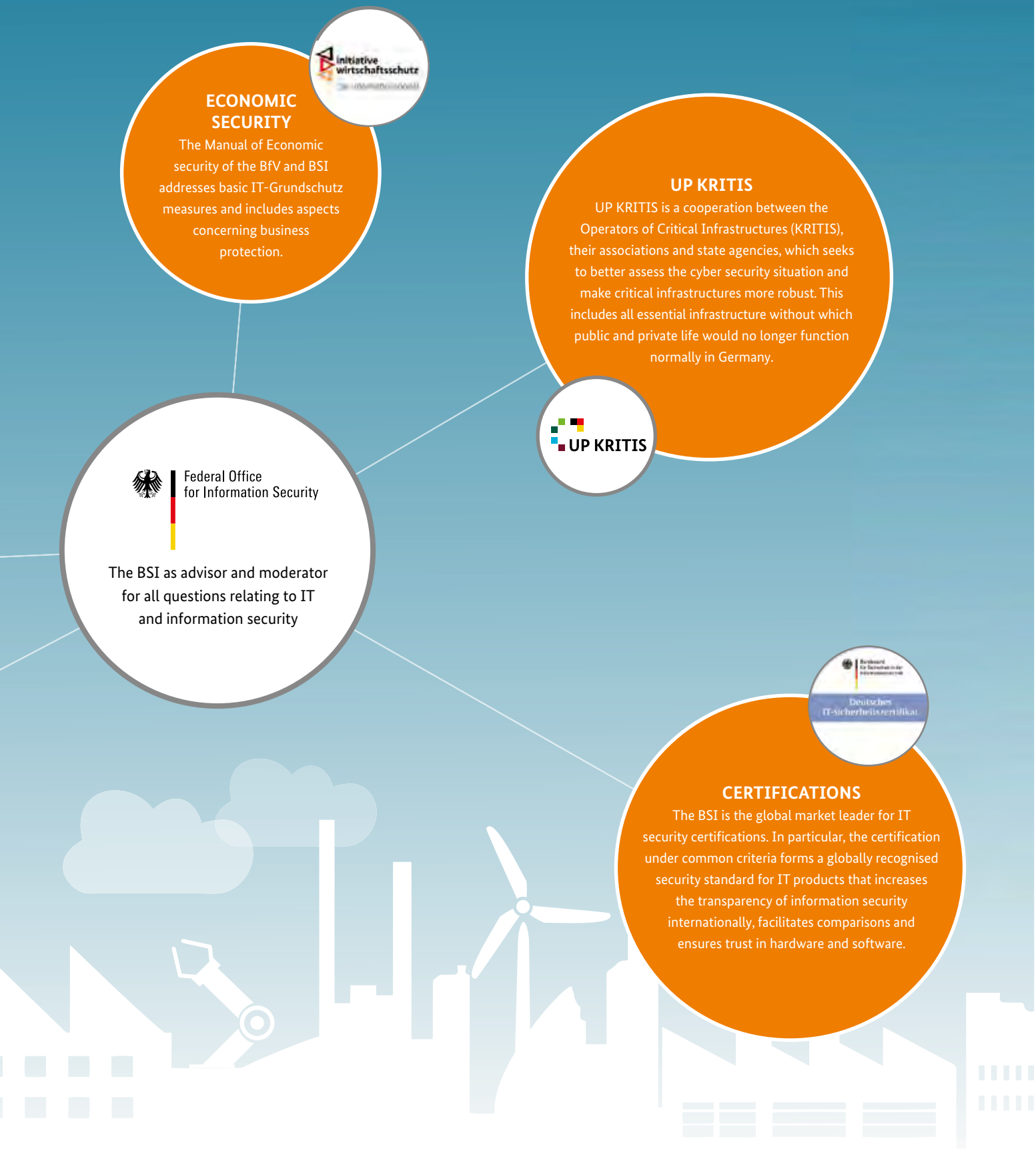
ALLIANZ FÜR CYBER-SICHERHEIT (ACS)

In collaboration with Bitkom, the BSI founded the Allianz für Cyber-Sicherheit in 2012. The largest national platform for cooperation on cyber security offers around 2,000 participants, 100 partners and 45 dissiminators extensive information on preventing and responding to cyber attacks. Focus is placed on how SMEs can apply relevant security measures. Participants benefit from cyber security conferences or regular working groups for open discussion.

IT-GRUNDSCHUTZ

With the IT-Grundschutz the BSI offers the most applied standard for information security in Germany – a collection of basic measures and protection programs for preventing and defending against cyber attacks, which is currently being updated.

German companies are distinguished by high-quality, innovative products – which is why they are an attractive target for cyber attacks. Almost all economic sectors and companies are affected, yet attacks are rarely detected. The government and business need to combine forces in order to combat this threat to the economy of Germany. As a neutral



body in its capacity as a national cyber security authority, the BSI shapes information security in digitalisation by means of prevention, detection and response for the economy. In doing so, it offers a range of information and cooperation options to strengthen the cyber security of German companies. ■

IT Security Knows no Borders

Interview with Bernd Kowalski

Digitalisation affects all areas of life, whether it's society, the economy or politics. The new digital technologies, products and processes are raising important questions – particularly for IT security. The challenge is especially evident in areas such as IT infrastructure in healthcare, the energy industry or autonomous driving in the automotive sector. Bernd Kowalski, head of the department for digitalisation, certification and standardisation at the BSI, explains the huge importance of IT security certification in digitalisation.

Why are certifications so important for successful digitalisation?

The advent of new technologies, driven by a dynamic market, always involves new security risks. These technologies must therefore be designed securely even before their launch onto the market. If this fails to happen, the security deficit may prove to be unbridgeable. Appropriate technical security standards and inspections by means of certification ensure that the new security risks brought about by new technology are minimised prior to market launch. This is because companies early on present their products to the BSI for certification, and are then able to safely launch them on the market once certification has been issued. The BSI issues IT security certificates for a range of different hardware and software products (including smart meters, network connectors in the e-health sector and statutory documents). Moreover, we also provide certificates according to technical BSI guidelines or the requirements of IT-Grundschutz.

However, it is evident that not all companies make use of the available certification. What could be the reason for this in your view?

Certification always entails a certain amount of time and cost expenditure. Secure, certified products are therefore typically more expensive than those without certification. Security is also a product feature, yet its economic benefit is not always clear to the customer and it is also often associated with a degree of inconvenience for users. This is why providers and users may sometimes see no direct benefit in certification.

How can this dilemma be solved?

This is where the state can play an important role: it can prescribe suitable provisions and framework regulations, as well as statutory technical standards and certification of the products affected. Indeed, the federal government has done so with, for example, the digital agenda. There are a whole host of digitalisation areas where we see a need for regulation and for the state to become involved in defining frameworks. In addition to the BSI's successful activities so far in the

Profile in brief:

Bernd Kowalski has been working for the BSI since 2002 and is responsible for digitalisation, certification and standardisation as the head of the department.

health, energy and ID systems sectors, this currently involves the automotive industry as well as finance and payment services in particular. The work we need to do in these areas is enshrined in the corresponding legislative provisions. Key importance will also be ascribed to Industry 4.0 or the Internet of Things which will be relevant to future industrial and social policy. For instance, the question arises of what tools can be used – alongside statutory regulation – to support the development of suitable standards.

'Meeting security requirements before new technologies enter the market'

What assistance can the BSI provide in this regard?

Today, certification in the BSI already covers a wide range of products for security-critical components. These are used in particular for secure identification, authentication and signature processes, as well as for secure online access and transactions. We are ideally positioned on the global market with regard to these products. In view of the rising demand for certified products, we also need of course to develop new processes, e.g. for standard products, which are applicable to the mass market and therefore beyond regulated sectors.

How can international requirements be satisfied by certification?

Companies nowadays expect us to provide testing requirements and certifications that can also be used on the international market. IT security knows no borders, which is why if we want to make technology secure and motivate companies to invest in this area, we cannot limit ourselves to the German market or niche areas. This is why we coordinate the requirements we develop in standardisation committees such as the Common Criteria Arrangement, as well as in technical committees at the European level such as the European Committee for Electrotechnical Standardisation and industry-led committees. This is how we seek to put forward our vision regarding IT security and develop the certification requirements defined with companies here in Germany into international standards.

What influence do legislation and regulations have at the EU level?

In the past, we primarily dealt with German laws such as the Personal ID and Passport Act or the Energy Act when it came to certification. However, we now have a growing number of regulations at the EU level. One example is the eIDAS Regulation for secure identification and digital signatures. It compels states to develop and prescribe relevant standards, and only to support those technologies that meet these requirements.

We work closely with other European partners in this regard – such as our French partner agency ANSSI, in many areas, they pursue the same goals as we do. By working together, we seek to establish our vision of security standards for regulations at a European level. In contrast to commercial providers, such as a number of global market leaders, here in Europe we want open security standards that benefit all applications. They should allow competition between various providers as well as the use of complex security technology by all users, and not be limited to a certain business model. Moreover, each country should be able to use the security standards in accordance with their own laws, societal values and economic situation.

For more information see https://www.bsi.bund.de/EN/certification

180 NEW MINDS FOR A COMMON MISSION

Shaping Digitalisation Security

Anyone who has the opportunity to visit the BSI at Bonn and look behind the scenes may be surprised: the atmosphere in no way reflects the dusty cliché of a public authority. Instead, it reflects the vibrancy of an innovative company based on exchange and networking among colleagues. It's no surprise though, because the close collaboration beyond areas of responsibility and departments forms an essential part of the BSI's success. Given the expanding remit, BSI employees can look forward to working with plenty of new colleagues who will join them over the course of the year. The agency is expecting the biggest staff expansion in its history, due to the approx. 180 vacant positions – roughly one in four faces in the offices, labs and meeting rooms will be new. But the right candidates still have to be found and recruited. We are therefore focused on the following question: what makes working at the BSI special?

The strategic decision to help give the BSI more clout by means of a major increase in staffing levels is based on the very clear fact that the risks facing the digitally connected world are constantly growing. Digitalisation is opening up unexpected opportunities – and it's clear that this requires increasingly complex technologies. This is leading to a rapid expansion in vulnerable targets for attack: as complete business models and processes are increasingly being moved online, the amount of programming code is also rising, as are the number of vulnerabilities. The growing networking involved in the Internet of Things, where billions of sensors and devices are already communicating with one another, likewise entails new areas of vulnerability. Theft of intellectual company property, the availability of critical infrastructures or the misuse of artificial intelligence to influence opinions using socialbots: digital technologies are advancing rapidly and are not only being used with good intentions.

ACTIVELY SHAPING THE SECURE DIGITAL FUTURE

One of the BSI's declared goals is to make the use of digital technologies a secure future opportunity for society, business, and government. Digitalisation will only be successful once cyber space can be made secure. This prospect holds great potential for many of us. Thomas Gilles, expert in 'Cyber Security for Digitalisation of the Internet of Things and Smart Services', embarked on his career at the BSI for this reason. 'Our job is all about finding constructive solutions,' Gilles explains. 'Anyone can get on here if they put in the work, and those who show initiative can also count on support.' In his rather challenging field, he particularly appreciates the proactive approach and teamwork. 'Professional confidence does come from being in an environment with so many experts. That doesn't mean however that I have to be able to do everything myself,' Gilles adds. Alongside the networked digital world, the experts at the BSI are also networking their talent and expertise in order to contribute to greater IT security with

'Anyone can advance here if they put in the work, and those who show initiative can also count on support.' ***Thomas Gilles***

effective solutions. Depending on the task at hand, Gilles therefore consults his expert colleagues with the relevant specialisation – and in contrast to the common perception of the public sector, takes the most direct route to do so.

FASCINATING RANGE OF ISSUES

The views expressed by Thomas Gilles are also shared by Jan-Hendrick Peters, an advisor in the 'CERT-Bund' section. 'I feel that I can make a real difference at the BSI,' Peters says. He emphasises the relevance of IT security in the age of digitalisation: 'Its huge importance stretches from areas of private life like online banking to future economic concepts such as Industry 4.0.' His day-to-day work consists of close contact with other national and international CERTs, IT security officers in administration and the economy, as well as citizens. 'What I find particularly interesting at the BSI is the variety of issues, as well as the rapid technological progress we are making with regard to both cyber attacks and countermeasures.' Full of passion and fascination for his profession, he also values the shared humanity that characterises the work in the cyber security agency: 'The BSI believes in a healthy work-life balance and also shows consideration for the personal concerns of staff.'

COMPATIBILITY OF WORK AND FAMILY LIFE

A comfortable working environment, coupled with challenging tasks, are also important aspects of work for Stefanie Euler, an advisor in the section IT Security Consulting for Public Authorities. When the mother of two started out in her career almost 15 years ago, she was considered something of a rarity, being a woman in this technical field. She is now all the more delighted to see a steady rise in the number of female technology experts. The BSI provides a work-life balance by offering the possibility of distance working, various part-time models and flexible working hours. This allows Stefanie Euler to stay on the ball even though she is employed part-time. 'The greater degree of flexibility has been hugely beneficial to me,' Euler explains. 'It also means I have enough time to

'I have always felt well supported by the BSI.'

Stefanie Euler

IT SPECIALISTS WANTED

The BSI will successively advertise around 180 vacancies over the course of this year. The authority is seeking information scientists, physicists, mathematicians and engineers – both university graduates (with bachelor's or master's degrees) as well as experienced professionals from MINT fields (mathematics, IT, natural sciences and engineering). Nevertheless candidates from other areas (for example, administration / economics or law) will also find interesting vacancies. Interested candidates can visit the new career portal at **https://www.bsi.bund.de/karriere** to find all the necessary information, from the vacancies currently offered to insights into working at the authority.

'I can contribute to something really relevant at the BSI. And that's a great feeling.'

Jan-Hendrick Peters

spend with my family.' But that's not the only important consideration for her: 'I am also completing a master's degree outside work to give me the opportunity to apply for a more senior position in the future,' Euler says. 'I had already received excellent support from the BSI during my earlier studies.' As is the case with Stefanie Euler, the BSI promotes the skills and talents of its staff, ensuring they are also well-prepared for the increasing demands of IT security in the future.

DIVERSE TASKS

The career paths, roles and backgrounds of the employees are so different and the areas of responsibility are so wide in which the BSI needs support. The focus is also on future technologies and risks making for exciting work in not only ensuring the digital future viability of the German state, the economy and society, but also inactively shaping these developments. Those tasks can be taken on in consulting, in cooperative boards, in the preparation of information, or in the operational cyber defense. The MIRT (Mobile Incident Response Team) is also being reorganised to analyse and clear up cyber incidents in particularly important institutions. In terms of prevention, evaluation of various sources is likewise being expanded in order to always maintain a current picture of the cyber security situation in Germany – a key requirement for improving the protection of government, the population and companies. This is also the aim of the networking of authorities and business – both with each other and beyond in the context of initiatives like the Allianz für Cyber-Sicherheit and UP KRITIS. There are also interesting challenges awaiting applicants in internal IT as well as press and public relations work. Altogether, these provide many good reasons for bright minds to join the BSI team. Just like Jan-Hendrick Peters did, who puts it in a nutshell: 'I find IT security so fascinating because it is critical for our digital future.' ■

'WE WANT YOUR DIGITAL PERSPECTIVE'

Tackling the skills shortage with a new approach to staff marketing: The BSI seeks to make suitable candidates aware of the professional opportunities at the authority. Besides the newly designed career portal, the BSI has launched an ad campaign, under the slogan 'Your digital perspective'. Nickolas Stöcker, recruiter at the BSI, notes, 'It emphasises that the BSI creates ideal and reliable framework conditions for its employees and their challenging and socially important work. This also includes the wide range of possibilities for organising work flexibly and according to the needs of family life.' Yet the BSI is an attractive employer for many other reasons. It enjoys an excellent reputation nationwide; it is highly respected internationally. Forward-looking security projects are part of our employees' everyday routine – everyone makes a significant contribution every day to greater cyber security for society. In addition to a fast-moving working environment, the BSI also offers its staff an extensive advanced training programme. Plus there are conferences and international project work, as well as regular discussion with leading security experts in Germany and around the world. Employees likewise enjoy first-class networking opportunities in politics, business and administration.

For more information see www.bsi.bund.de/karriere und bewerbung@bsi.bund.de oder unter Tel.: 0228 99 9582 0

Cooperation between the Federation and States

By Arne Schönbohm, President of the BSI

Working Together for Greater Cyber Security in Germany

Digitalisation is becoming an ever-present issue in both federal and state authorities, in the operational and administrative areas of governance. For instance, this is evident in processes like official file management, which is increasingly being handled electronically. The benefits are clear: higher efficiency, falling costs and a reduced bureaucratic burden. At the same time, dependence on properly functioning information technology is rising. In practice, many authorities are aware of the serious consequences an IT outage can entail. An increasing number of authorities are therefore introducing information security management systems (ISMSs).

Nonetheless, internal oversight for information security will not be sufficient for the long term. No public authority is an island; digital transformation will not stop at city or national boundaries. In contrast, the benefits of digitalisation may only be fully realised once it becomes established across different authorities. Therefore, the goal is to establish a minimum level of security whilst various authorities become increasingly connected. In its capacity as a steering committee, the IT planning council therefore passed the 'Guideline for Information Security' in March 2013 between the federation and states. The BSI plays its part with discussions in the information security working group (AG InfoSic) as well as in the sub-working group for information security management (UAG ISMS). This resulted, for instance, in a collection of blueprints and resources in the UAG ISMS that are used to support the appointment of an IT security officer and the introduction of the ISMS. This approach helps authorities at the start of their information security process to establish clear information security structures.

Alongside AG InfoSic, the Administrative CERT Association (VCV) was set up for exchanging information at the level of

'It is clear that cooperating at the state and federal level results in a 'win-win' situation that leads to an overall increase in the level of cyber security in Germany.'

the Computer Emergency Response Teams (CERTs) of the federation and states. Besides two meetings per year where experience is discussed regarding operations, the cooperation particularly emphasises the swift exchange of warning notifications. In this connection, around 2,000 warnings were distributed to subscribers last year using the CERT-Bund's warning and information service, based at the BSI. The police forces of the federation and states have also regularly exchanged information regarding the protection of information in police information networks since 2004. The BSI provides support in this context by exchanging technical expertise which is then incorporated into requirements for safe Internet use at the workplace in relation to police organisations.

It is clear that a successful cooperation between the federal and state authorities results in a 'win-win' situation that leads to an overall increase in the level of cyber security in Germany. Only a holistic approach can bring about cyber security. With the cyber security strategy for Germany published in November 2016, the BSI has intensified cross-level cooperation that envisages the closer involvement of states in the further development of the German cyber security architecture. This is currently evident in the expansion of the BSI Act. This is designed to enable the BSI to support German state governments – at their request – in matters concerning defence against risks to security in information technology. As the cyber security authority for all of Germany, the BSI has thus obtained a mandate to further expand its offering and services for the state governments.

By developing networked communications within the BSI, new target groups should be developed in the states and municipalities, while existing interfaces will continue to be developed with respect to addressing key partners more quickly and seamlessly. The goal is to bring together expertise and exchange knowledge for all involved, making it available from a central point. This is needed due to the fact that any fragmentation of cyber security resources would pose a serious risk to Germany's security architecture.

Digitalisation holds much untapped potential, but in developing this potential, cyber security measures should be developed and implemented by the federal and state authorities using their combined expertise. The BSI will therefore act as a major centre for knowledge and expertise, at the same time shaping information security in Germany for the federal states. ■

15 YEARS OF BSI FÜR BÜRGER

Combatting Digital Carelessness

Digitalisation is penetrating more and more areas of daily life. Conversely, cyber attackers are continuously honing and developing their attack techniques at a rapid pace. Cyber security has therefore become one of the key challenges of our time. Autonomous and safe activity in cyber space is likewise becoming increasingly important – and not just for the state and economy, but for citizens too. An initial step for dealing with cyber hazards is being aware of the risks.

The BSI accepts its responsibility to inform and raise awareness among citizens for the safe use of information technology, mobile communications and the Internet. In doing so, the BSI enables citizens to act responsibly and be aware of the risks in cyber space.

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

www.bsi-fuer-buerger.de ▪ www.facebook.com/bsi.fuer.buerger

CD-ROM from 2002

The first website in 2003

Since **2003** a wide range of information has been available on the website www.bsi-fuer-buerger.de. It covers topics such as online banking, smartphone security, e-mail coding or social networks and includes recommended actions, explained clearly for technical laypeople.

In **March 2002**, the information service BSI für Bürger was launched with the support of the Federal Minister of the Interior Otto Schily under the slogan 'Onto the Internet – safely'; it came in the form of a CD-ROM, over 650,000 copies of which were distributed in the first year alone. Due to the great demand and the ongoing need for updates, the BSI set up soon afterwards the online portal www.bsi-fuer-buerger.de.

https://www.bsi-fuer-buerger.de today

In **November 2015** the website was completely overhauled. Interested internet users now have access to even more up-to-date information, in a stylish and user-friendly interface. The fact that the website has been well-received is shown by the rise in website views from an average of over 151,000 visitors per month in the period from July 2014 to June 2015, to an average of over 172,000 visitors per month in the period from July 2015 to June 2016.

- With 'Bürger-CERT', the BSI offers a free warning and information service that provides quick, expert information on areas of weakness, vulnerabilities and other risks, as well as helpful advice. BSI experts therefore analyse the security situation online and send out notifications to currently more than 100,000 subscribers whenever there is need for action. Moreover, the e-mail newsletter 'SICHER • INFORMIERT' highlights the key security news items every fourteen days.

- The BSI provides information and communicates with citizens via its Facebook page (www.facebook.com/bsi.fuer.buerger) as well as its Twitter channel (www.twitter.com/BSI_Presse), which has been active since March 2016. On 31st January 2017, these channels were followed by 28,129 fans (Facebook) and 4,729 followers (Twitter).

- Private users can also contact the BSI Service Centre for any questions they have on IT and internet security – indeed, around 400 users do so each month.

Offering all these information services, the BSI sees itself as an expert, independent point of contact for cyber and IT security that aims to bring these issues to the public's awareness, thus combatting digital negligence. Among the many European authorities and institutions, it is quite unique in this regard.

IT SECURITY
IN PRACTICE

Security by Design:

eID GATEWAY

Universal Communication in Industry 4.0

By Dr Andre Braunmandl, section Cyber Security for Digitalisation in Transport and Industry 4.0
and Dr Dennis Kügler, head of section Chip Security Analysis

The BSI conducts a cyber security survey every year. In 2016, over half of the institution surveyed stated that they had already experienced successful attacks. According to statements provided, almost all of the victims suffered tangible losses, and some respondents reported significant consequences for their institutions.

CYBER SECURITY FROM INDUSTRY 3.0 TO INDUSTRY 4.0

The availability and reliability of IT systems are of essential importance, and this is particularly true in the industrial sector. Industry 3.0 is already characterised by a high degree of IT penetration, enabling far-reaching automation. Successful attacks on individual IT systems therefore result in rather isolated outages or faulty production steps. The transition to Industry 4.0 brings with it an ongoing networking of IT systems, both within the company and externally via the Internet. This ongoing networking drastically increases the area of attack for cyber criminals and industrial spies. Traditional perimeter protection and mutual partitioning between relevant departments and companies are completely inadequate in this respect. For Industry 4.0, the systems themselves need to be better, and also be able to inherently protect themselves, in order to be able to implement effective measures by financially justifiable means if there are acceptable residual risks.

This means that, in Industry 4.0, the focus is not only on the traditional requirements of availability and operational reliability of production systems, but also the traditional IT security objectives of confidentiality, integrity and authenticity for all networked production components as development objectives. As a result, there is a conflict of objectives, as the very principle of these additional IT security goals is based on restricted availability. If, for example, an authentication key can no longer be used due to their certificates expiring, it is no longer possible to use the system to renew the certificate, or this can only be done with restrictions.

STANDARDISATION AND CERTIFICATION FOR INDUSTRY 4.0

In order to simultaneously guarantee a high level of security and high availability, it is essential to standardise and certify security-relevant components and services.

The key basis for this is the introduction of an overarching authorisation concept on the basis of integrated management of all participating electronic (machine) identities (eID management). From a technical perspective, these can be flexibly and scalably realised through building an overarching Public Key Infrastructure (PKI), in combination with the secure storage and management of eIDs on the relevant machines. To this end, the BSI is currently designing an eID gateway using a generic approach, which supports a standardised security concept across all levels of traditional automation pyramids (Fig. 1) and which is to be used on all of these levels.

The central element of the eID Gateway (Fig. 2) is a certified security chip (security element, SE), which functions as a hardware security anchor. Certifying the hardware ensures the secure generation, storage and utilisation of keys for

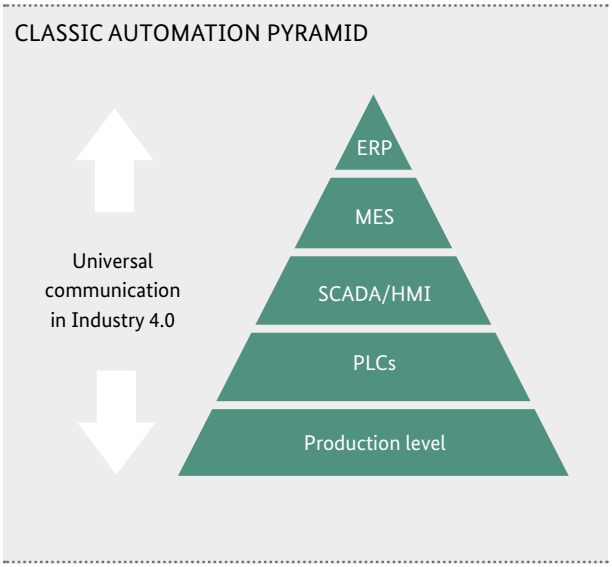


Fig. 1

the cryptographic methods in use. The fundamental requirements for security elements are currently defined in the technical guidelines and protection profiles set out by the BSI. As these chips are intended to support use scenarios from the mobile and device to the HSM at server level, the scalability mechanisms (by means of parallelisation) and availability (e.g. by means of redundancy) are of huge importance. A clear separation between application and security functions in combination with a flexible certification concept means that a basic security chip that is certified once can be used in a wide scope of applications, which in addition to Industry 4.0 may also cover, for example, automotive security, Vehicle2X communication or even use in cash registers. Its wide scope of application means that the chip is cheap and cost-effective to use.

THE eID GATEWAY IN USE

In order to control the eID gateway, the BSI specifies a uniform interface (application programming interface, API). This API should meet a range of requirements. Initially, the API should allow access to security elements and the software crypto libraries by means of a standardised interface, which supports advanced Industry 4.0 communications standards such as OPC UA. The application programmer should therefore be able to concentrate on the application, which accesses its security functionalities via the eID gateway regardless of the SE specifically used. The intention is therefore to transfer as many IT security aspects as possible into the scope of the eID gateway. The role of the eID gateway administrator may then be transferred to a specific IT security specialist, or to a certified service provider. In practice, it has been apparent to date that industrial systems application programming and IT security are areas that are so diverse and demanding that a single person cannot have expert knowledge of both.

The eID gateway therefore takes on the role of a universal security provider for Industry 4.0, performing the tasks of authentication and confidentiality as well as providing integrity protection for machine communication (M2M communication) in the industrial environment. Its standardisation allows for a broad scope of use and provides a comprehensive and cost-effective security approach. ■

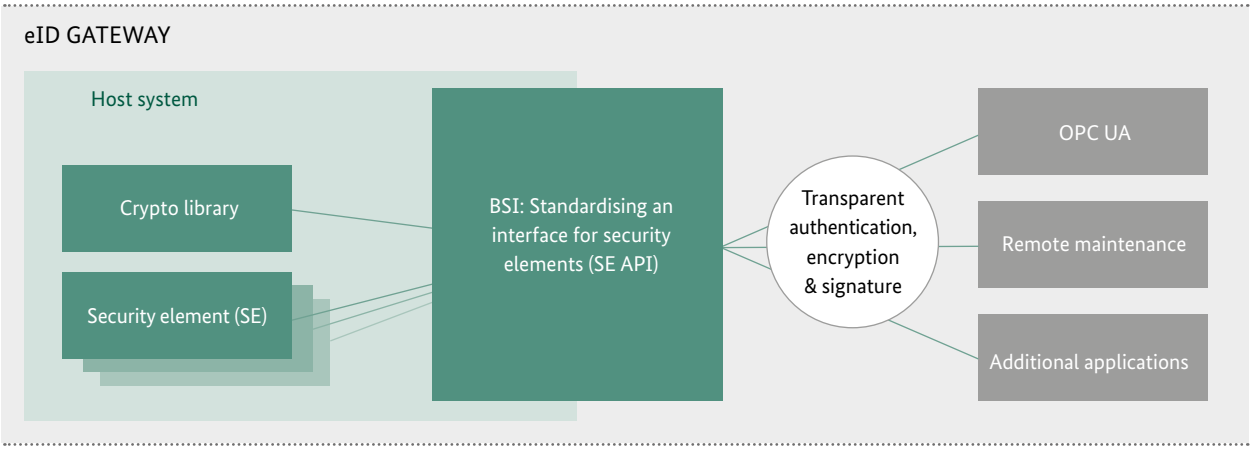


Fig. 2

Mobile Identification: Making it Secure

By Dr Ulf Löckmann, section eID Applications in E-Government
and Ingrid Grüning, section Cyber Security for Digitalisation in the Public Health and the Financial Services Sectors

Electronic Identity Verification

Whether opening a cheque account online, buying a SIM card or acquiring De-Mail access: in the digital world, identifying the user in advance is a statutory requirement for many services. This not only results in rising demand, but also an uptrend in the options available for online identification.

ONLINE ID CARDS WITH THE PERSONAL ID CARD

The German personal ID card has been a secure and highly trusted method of online identification since 2010. However, the services available with the eID function have not grown as quickly as demand for user-friendly solutions.

The increasing need for online identification has resulted in a market in Germany for remote identification services. In accordance with the Money Laundering Act, after opening an application, identification service providers are also increasingly offering processes that use video chat for identification with the personal ID card. Many banks now rely on video identification as a quick alternative to traditional processes such as PostIdent.

However, the most that can be achieved via a video channel is checks on security features such as the holographic portrait or the laser image on the reverse, which change in certain light conditions when the ID card is moved. This means, however, that the authenticity and originality of an ID card can only be checked to a limited extent by video link. And, as video transmission is also always susceptible to technical manipulation, it is the opinion of the BSI that this type of process does not achieve the required security in order to allow reliable identification, as is possible face-to-face or with the eID function.

INCREASED NEED DUE TO THE eIDAS REGULATION

In order to 'enable secure and seamless electronic interactions between businesses, citizens and authorities', the European Union issued the eIDAS Regulation in 2014.

Since 1 July 2016, this has governed electronic trust services, such as for qualified electronic signatures and timestamps and the issuing of electronic registered mail. And it is precisely services such as these that require reliable user identification. It stands to reason here that processes free of media disruption should also be permitted, as they can be performed without a time delay.

The eIDAS Regulation itself also provides an option for online identification: The member states of the EU are able to notify their own electronic identification systems, which need to be recognised in other member states. In this process, the level of trust achieved in each case is stated for each identification system, i.e. low, substantial or high.

THE FUTURE OF THE eID FUNCTION

Notification at a high trust level is envisaged for the eID function of the German personal ID card, and of the electronic residence permit, as it already fulfils all corresponding requirements. This means that in future it will be possible to use the eID function for secure identification EU-wide.

In order to promote marketability and the use of the eID function as a secure means of identification, the Federal Ministry of the Interior has tabled a draft law. An additional aim of this is to significantly reduce the hurdles for service providers. For example, the draft envisions a simplified application process for authorisation certificates, and the eID function will be used in principle for newly-issued ID cards.

At the same time, the BSI is upgrading the technical usability of the eID function: the mobile version of the AusweisApp enables the eID function to be conveniently used from a suitable NFC-enabled mobile phone, no longer requiring a separate scanner.

THE SUITABILITY OF DIFFERENT PROCESSES

Regardless of the process chosen by the user for identification, what is essential for the user's confidence in this process is a uniform perspective at the corresponding level of trust, on which the user and supplier alike must be able to rely, as is the case for supervisory authorities and the legislator.

The BSI has compiled a Technical Guideline for assessing the security level of huge authentication processes with a standardised method. This makes it possible to select a particular level of trust (in accordance with the eIDAS Regulation) from various, equally suitable processes. The Guideline can be used, for example, as a basis for consistent checking by accredited compliance assessment offices. This creates legal certainty for service providers and avoids the need for additional application-specific requirements. It is then only necessary for specialist laws to define what trust level is required in each case and for each specific purpose. ■

The AusweisApp 2 is available as a beta version for android in the Google play store:

For more information see https://www.bsi.bund.de/dok/8925166

Ten Years of DsiN: An Interview with Dr Thomas Kremer, Chairman of the Board of Deutschland sicher im Netz e.V.

DsiN recently celebrated its 10-year anniversary under the tagline 'Security comes from responsibility'. What are the most important milestones that the association has achieved since it was founded?

Deutschland sicher im Netz e.V. was founded in 2006 at the National IT Summit as a joint initiative between business, politics and society, in order to increase awareness of IT security among consumers and companies. At that time, only 50% of the people in Germany used the Internet. The smart phone, as we know it today, only came to market one year later – and the Internet economy was still in its infancy.

Today we have a significantly more networked world, and with that comes a greater need for better education. New DsiN services relating to both networked mobility as well as protection-related knowledge in schools are evidence of this change. However, even standard issues continue to be current: As long as 'hello' or '12345' are among the most frequently used passwords, we have to keep educating on the issues.

To date, we have reached over 10 million people. For us, the first priority is to motivate people to change their behaviour and to try to understand how to behave securely online. This requires a professional and patient approach, and strong partners: our members and partners form the basis for initiatives, in particular the expertise of the BSI as well as support from the Federal Government, and first and foremost our patron, the Federal Minister of the Interior. His steadfast commitment to DsiN at our anniversary conference was very symbolic for us.

What is the foundation of the explanatory work performed by the DsIN?

The foundation of our work is the DsiN Security Index, which relates to the security situation of consumers in Germany. It summarises the security situation in one key indicator. At the same time, it defines security requirements by four consumer groups, which are the basis for our explanatory services: the fatalists, outside users, trust users and master users. The next survey will be published at the end of May 2017. Each individual group means different challenges for us in our attempts to educate.

What are the hurdles in your attempts to educate – and how do you deal with them?

It's about really reaching people. Using the findings from the DsiN Security Index that we just mentioned, we react to specific security requirements as well as motivations: for example, the fatalists are people, mostly younger, who have an uncanny knowledge of how they can protect themselves online, but ultimately do not put that protection in place because they firmly believe that there would be no point in doing so. We work against this fatalism through programmes such as the myDigitalWorld youth competition, in which we motivate young people to engage with digital protection, and even develop their own ideas in this area. For the group of outside users, which includes an increasing number of

'The BSI is an important partner to us in furnishing explanatory services with the required expertise.'

Profile in brief:

Dr Thomas Kremer is the Chairman of the Board of Deutschland sicher im Netz (DsiN), and a member of the Board of Deutsche Telekom. DsiN offers small and medium-sized enterprises and consumers alike specific assistance in how to behave securely online. A decision was made in the Federal Government 2016 Cyber Security Strategy, to continue the educational initiatives with DsiN. DsiN is a non-profit organisation under the patronage of the Federal Minister of the Interior, and has its registered office in Berlin.

older people, the challenge is not the lack of will, but a continued lack of knowledge in this area. Here, we start with the materials that Digital-Kompass provides for workshops; in fact, we often start with the absolute basics. The group of master users again has a lot of knowledge and also applies it. These people are of particular interest to us at DsiN as disseminators of knowledge. As we are currently doing in the digital neighbourhood for example, we want to pass on their knowledge and experience to other people.

■ Collaborative partnerships play an important role in DsiN's work – why are these partnerships so important? What role does the Federal Office for Information Security play?

The BSI is an important partner to us in furnishing consulting services with the required expertise. For example, among small and medium-sized businesses, we often refer to BSI's IT-Grundschutz and consult experts. In this interaction between DsiN and various partners such as the BSI, the magic formula consists of speaking the language of consumers and looking at IT security from their perspective, meaning that we can contribute to the spread of expertise and putting it to best use. In general, we maintain partnerships not only with experts such as the BSI or the Fraunhofer Institutes, but also influential partners from civil society such as the senior citizens organisation BAGSO or the Claims of Commerce and Industry for small and medium-sized businesses – and are always open to new partnerships.

■ What issues do you believe are critical in IT security, and in your opinion require greater explanation, in particular with regard to dialogue with policymakers and business?

The DsiN 2016 Security Monitor shows that most companies today have basic protective measures as well as antivirus protection. At the same time, there is a lack both of awareness of and expertise in integrated protective concepts. There is also a deficit in the implementation of organisational measures, such as when it comes to social engineering as a gateway for cyber criminals. A great deal of education is still required in this area.

Of course, there are also limits we keep to with respect to educating the public: Here, we have to speak to business providers – or even work towards mandatory requirements for users. Encryption is a good example. There are now good initial indications that business is providing simple and secure solutions in this field.

■ What are your plans for the next 10 years of DsiN?

Digital expansion in all areas of life is accompanied by a need to explain to consumers and companies how to remain secure. We want to make our presence felt here, to be a point of contact to provide practical help and guidance. We of course invite companies and partners to continue on this route in future through joint initiatives, and to keep pushing it forward. The commitment made by the Federal Government in the Cyber Security Strategy that it would promote DsiN's educational initiatives also supports this objective. ■

THE SECURITY BAROMETER

The security barometer (or 'Siba', short for 'Sicherheitsbarometer' in German) provides updates about the current IT security situation as well as providing tips and assistance in avoiding risks online. Siba identifies risks on the Internet based on a traffic light principle, and in this way helping users to assess risks. The service is provided by DsiN in collaboration with various partners such as the BSI.

Siba is available as an app from all the usual app stores, and can also be downloaded from www.sicher-im-netz.de/siba.

DIGITAL PIRACY

By Joachim Gutmann, Glückburg Consulting AG

Cyber Attacks in Maritime Transport

Profile in brief:

Joachim Gutmann is a freelance journalist and author. His professional career has been spent in Berlin, Bonn, Düsseldorf, Gummersbach and Hamburg. He has spent the last 17 years working as a communications expert for Glückburg Consulting AG.

A container ship from Latin America is being unloaded in Rotterdam. The process involves individual containers being unloaded separately, placed onto a waiting truck trailer, and immediately driven off. A few days later, the shipping company realises that someone had penetrated the computer program externally, and organised the coup. The content of the container is a matter of speculation.

'It's one example of many,' comments Lars Lange, General Secretary of International Union of Marine Insurance (IUMI), the international transport insurance association. 'There are even more cyber losses today than we think.' Whether it's the navigation systems on the ship's bridge, drive systems, internal communication, additional system leaks or documents relating to individual containers, with every new build, even more information technology comes on board.

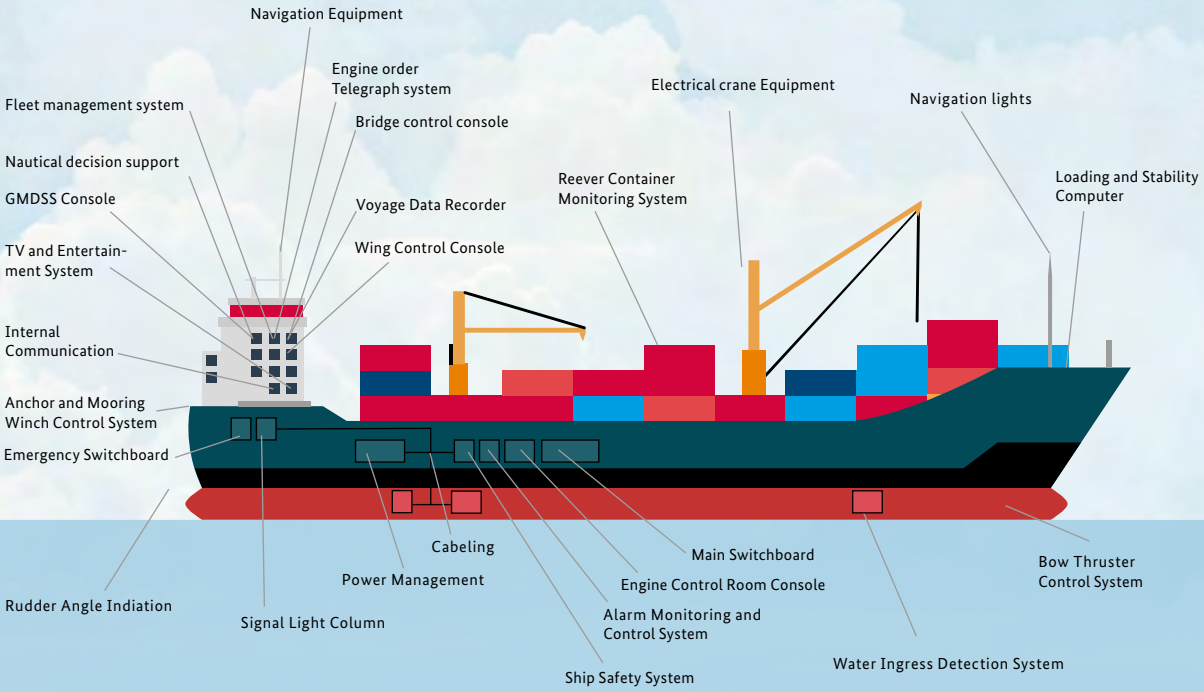
'The ship is a floating data centre,' says Jan Hinnerk Haul, IT expert at the classification company DNV GL. This data centre can be attacked. The US Transport Ministry has collected a total of 26 attack points. Back in 2013, researchers at the University of Texas proved that a ship can be steered externally. GPS data was manipulated to achieve this, and the navigation systems on board did indeed incorrectly calculate the position. The worst-case scenario is a meltdown. The danger is entirely real, as the ECDIS (Electronic Chart Display and Information System) navigation system used on board not only makes a ship susceptible to faults, but also connects to the Internet, making it a gateway for computer hackers.

Cyber danger lurks not only at sea but also on land. Access systems, cargo handling and crane control systems, as well as the SCADA software used in many systems make the harbour a physical cyber system, and one that is poorly protected at that. According to a report by the Baltic and International Maritime Council (BMICO), the world's largest maritime organisation, an examination of 20 container ports found that 16 locations had 'serious vulnerabilities'.

Shipping companies are also spied upon in order to find out which ships are carrying a valuable load, and are also subject to less surveillance. According to a recent survey by the Weltreederverband (2016), 21% of respondents stated that they had been victim of a cyber attack, while 57% said they had not and 22% did not provide an answer. They reported data loss (48%), financial losses (21%) and limited IT functionality (67%). Only 4% reported an attack on ship systems, and only one in four shipping companies had considered defence systems. 'That is too few,' says Lars Lange. 'The shipping companies don't want to see the risk.' Although no ship has been lost thus far due to a cyber attack, it is surely only a question of time.

Maritime industry associations BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO do not just want to wait it out. They agree: it is time for cyber security on board ships. At the beginning of 2016, they published instructions to improve cyber security on ships – from cruise liners to freight ships to tankers. The guidelines are based on internationally recognised frameworks such as the Cyber Security Frame-

POSSIBLE ATTACK TARGETS FOR CYBER CRIMINALS



ICS Security in Maritime Transportation, U.S. Department of Transportation

work published by NIST, and includes maritime security standards such as the ISM Code and ISPS Code. Their objective is to create generally binding technical rules and give regular training to the crew on board.

These regulations are compulsory: The more the linking of control and navigation systems progresses with additional networks and entertainment systems, the easier IT interfaces make it for third parties to access company networks along this chain. Shipowners believe they are in the clear, because to date it has not yet been possible to create a stable connection to ships across all the seas and oceans. In addition, the systems on ships for operating and steering should be separated from those used for communication. This should increase security, as should virus scanners and firewalls in the communications systems on board.

However, Prof. Thorsten Blecker from the Institute of Business Logistics and General Management at TU Hamburg, believes that the greatest source of danger lies elsewhere, namely in unmaintained Programmable Logic Controllers (PLC), which are used to control or regulate a machine or system and are programmed digitally, and which are in fact connected to the Internet without any protection. Their long service life (up to 25 years), outdated protocols (some of which do not have any security features), and the problem of installing patches (due to availability) make them a security risk. “We also need IT security management in the maritime transport sector,’ says Becker.

However, Jan Hinnerk Haul believes that more training and greater awareness are the key. He complains of a flood of email from shipping companies to ships, the gateway for malware, as well as the uncontrolled use of USB sticks and a lack of antivirus systems. The International Maritime Organization therefore states that shipping companies urgently need to train members of the ship's crew in the use of online social media. There are also complaints that most ships – apart from large ferries – do not regularly have specialists in electronics or information technology on board. In the context of the current level of threat, this needs to change – and quickly. ■

Secure Passwords

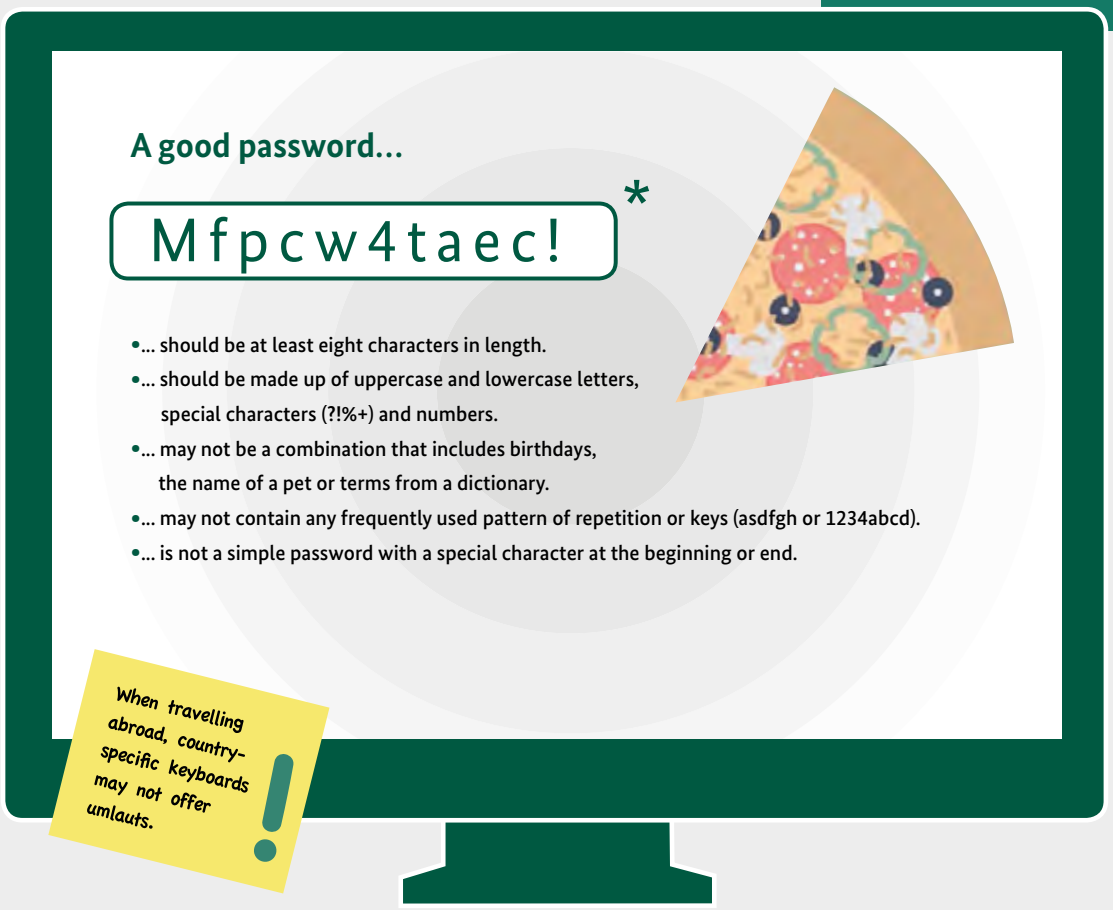
A Basic Tip from the BSI

Treat passwords for your e-mail account, social networks and your computer the same way you would treat your house keys: The only way to protect against unwanted guests accessing your personal data, photos or account information is to have a secure password.

And the principle that applies to your house keys is exactly the same for a virtual key: the more complex it is, the more difficult it is to break the lock.

Working with passwords

- ☑ Keep passwords under lock and key
- ☑ Update passwords regularly
  Change time intervals
- ☑ Do not use the same passwords for multiple accounts
- ☑ Change preset passwords
- ☑ Do not pass on your passwords to third parties and do not send them by e-mail



*) ***The mnemonic:*** *Noting the first letters of each word in the sentence is a really easy way to remember a password with more than eight characters. That way you are very well protected. To take a German example, 'Am liebsten esse ich Pizza mit vier Zutaten und extra Käse!' (or 'My favourite pizza comes with four toppings and extra cheese!') makes the password: AleiPm4Z+eK! That way you are very well protected.*

For more information see https://www.bsi-fuer-buerger.de/Passwoerter

COUNTER-ESPIONAGE THROUGH EMISSION PROTECTION

By Dr Amin Hellerbach, section Emission Security

If you hear the word 'IT security', malware, vulnerabilities, hackers, phishing mails and botnets generally spring to mind. Aside from these ever-present risks to IT security, there are other, less obvious routes down which critical information could leak. One of these routes is based on the use of physical effects and is known as 'compromising emanations'.

WHAT ARE 'COMPROMISING EMANATIONS'?

Even if we are not able to perceive it in our everyday lives, we are constantly surrounded by electromagnetic fields, wherever we go. All kinds of electrically driven devices radiate these fields and trigger effects, some of which are unexpected. Thanks to the consistent implementation of guidelines relating to radio interference suppression and electromagnetic compatibility by industry bodies, this mostly remains unnoticed and free of consequences, even if the occurrence of curious phenomena is not ultimately ruled out. For example, the function of pacemakers can be so disrupted when in the vicinity of large electrical systems that it could result in the death of the wearer. Measures aimed at radio interference suppression reduce the strength of emitted electromagnetic fields such that disruptions are no longer expected, but the fields are not eliminated. It is therefore still possible to capture, assess and reconstruct information from the emissions from an IT device. If government secrecy is at risk from this process, this is referred to as 'compromising emanations', or TEMPEST.

THE THREAT SCENARIO

If a high level of protection is required for information to be processed electronically, a specific decision is often made to disconnect from the Internet, and therefore withdraw the basis for all attacks that come from the Internet. Under these very conditions, compromising emanations are an effective, clandestinely and widely used attack vector. Critical data is captured in this process, either before it is encrypted, or after it is decrypted. If, for example, a text file is transported in encrypted format, it is seen at the latest in clear text on the editor's screen. A potentially con-

Representative image of a emission test booth

fidential reply is entered using the keyboard, as is done for other passwords. All of this equipment emits radiation and therefore becomes a security risk without being perceived as such. A technically well-versed attacker can conceal an appropriate probe outside the monitored security area, in order to capture emitted signals. As this type of bugging is entirely passive, the attacker has few worries about being discovered.

COUNTER MEASURES TAKEN BY THE BSI

In order to keep expenses to a reasonable level, the BSI focuses on prevention for minimising risks due to compromising emanations. The basis for action is formed by administrative specifications for the protection of classified information, which the BSI is in charge of generating in the national framework. As the 'National TEMPEST Authority', the BSI also actively helps to shape this in an international context within EU and NATO committees, and is responsible for approval specifications. If confidential information with a classification higher than restricted is processed, the relevant IT systems must first successfully undergo an extended certification process. In the field of emmission safety, this covers practical measurements of the emissions characteristic of a device. For this purpose, the BSI has notification-based test laboratories for systematic and replicable testing. In the case of large objects, such as ships and aircraft, radiation testing is also carried out on site.

PRACTICAL IMPLEMENTATION

The BSI supports a range of companies which specialise in upgrading standard IT devices with shielding. In order to verify the effectiveness of this shielding, any device that is reinforced in this way undergoes a radiation test and its individual emissions characteristic ('fingerprint') is created. In the event of a re-test, e.g. if there is suspected tampering, changes which may have been made by, for example, an attacker can then be detected. If the device successfully passes all tests, it is given a seal which acts as verification and also detects tampering. It is then certified for use in processing classified information according to its radiation properties.

The TEMPEST device manufacturers supported by the BSI are authorised to carry out radiation testing. Certification using a sample device is only conducted by the BSI; the manufacturers then perform the radiation tests for their series production using a test method specified by the BSI. ■

TL-03305

In Technical Guideline TL-03305 lists the TEMPEST device manufacturers supported by the BSI, and their products which have already been awarded certification. This can also be done for customised devices if requested or required by a consumer. A case such as this can be handled by one of the listed manufacturers, which closely coordinates all certification issues with the BSI.

For more information see https://www.bsi.bund.de/dok/6800054

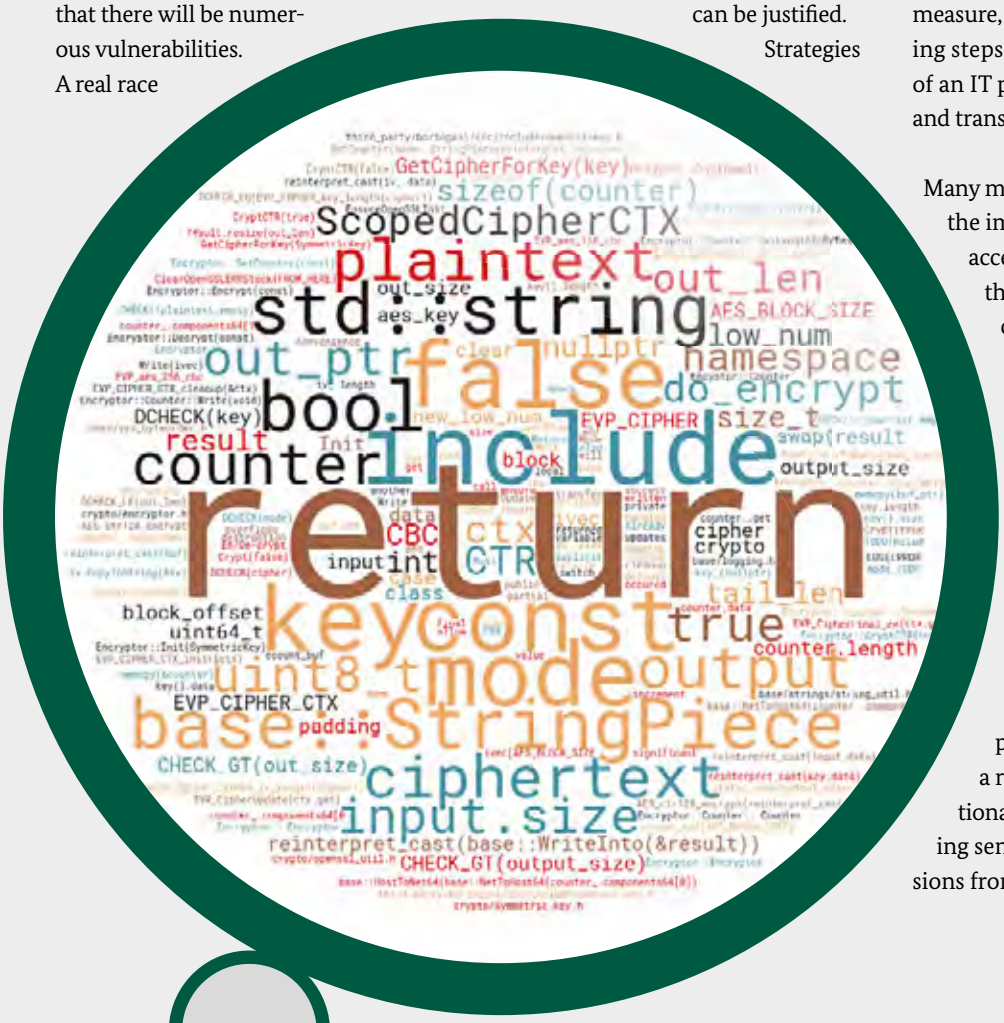
SOURCE CODE TESTING AS A BASIS FOR TRUST

By Oliver Zendel, head of section Evaluation Coordination and Methodology and Thomas Caspers, head of division Evaluation and Operation of Cryptographic Systems

Leading edge IT products need an appropriate, needs-based and therefore often ever-increasing range of function. This has a direct effect on the complexity of products. Indeed, they are usually now so complex that it is statistically probable that there will be numerous vulnerabilities.

A real race has developed between attackers and defenders as to who can find these vulnerabilities most quickly. Therefore, when software is used for security critical government applications, the question always arises of how unshakeable confidence in IT products can be justified.

Strategies for answering these questions must also have the aim of finding analysis methods for deliberately or unintentionally detecting errors and vulnerabilities which have crept into source code. The direct analysis of source code plays a key role here as a preventive measure, as all functions and processing steps and the internal structure of an IT product are only complete and transparent on this level.



Many manufacturers now recognise the importance of controlled access to source code, in order that they can meet the increasing demand for trusted certification. Major manufacturers have therefore established methods to enable third-parties, e.g. governmental bodies, to test source code (see box). Free-licence software always provides source code analyses of any depth at any time, and under any conditions. In contrast, proprietary products series face a range of technical, organisational and legal challenges drawing sensible and reliable conclusions from examining source code.

For analysts who need to draw conclusions about trust, specific knowledge of the architectures used by manufacturers and technicians form the key requirements for successful testing. Further to this, it is vital that source code analyses can be performed on complex products using technically advanced and freely available tools. Purely manual source code inspections, e.g. simply 'reading' the code, with the exception of very detailed inspections of specific product characteristics, draw almost no conclusions about the product as a whole. The use of tools for analysis, which allow much of the testing to be automated, is not necessarily is not necessarily the first choice of manufacturers of proprietary products, as the requirements associated with this can in practice be highly complex and mean increased costs. In the international arena, complex legal circumstances may be involved.

Along with comprehensive access to the actual program code and the related documentation, the availability of sources for the latest stable version, including the latest security updates, is of key importance to the BSI. Replicable builds then create a testable path from the sources to the binary files. For this reason, the involvement of compiler, linker and method of code signing plays an increasingly important role. This is the only way to ensure that the tests actually relate to the binary files that are subsequently used.

Normally, IT manufacturers limit access to source code, if they do not publish under free licences, to premises which are fully under their own control. In such circumstances, in-house analysis systems are needed to perform proper, independent analysis. The manufacturer must allow such systems to be synchronised and used by the testing authority.

The Experience of manufacturers who have a genuine interest in the in-depth and consistent trust certification of their products, shows that successful and profitable source code analyses can already be implemented today. If there are no suitable and adequate levels of certification for a software product according to common criteria, which already include reliable conclusions, then specific source code testing represents a pragmatic approach to drawing these conclusions regarding trust. Of course, this cannot prove that a piece of software is really completely free of both errors and vulnerabilities (and indeed that is not the actual purpose of such testing). Particularly critical aspects, such as the generation of random digits, and the integration and configuration of libraries for encryption or authentication, can, however, be properly tested if the source code is available. This is highly beneficial to the manufacturer of an IT product, since reduced error rates lead to falling costs in the product cycle. All users of the product also benefit from enhanced security features. The consistent performance of source code analyses is paying dividends in the form of promising approaches to transparent trust certification and better quality solutions for use in critical environments, such as the information technology used in government communications. ■

MAJOR IT MANUFACTURER PROGRAMS FOR INSPECTING SOURCE CODE:

APPLE OPEN SOURCE
https://opensource.apple.com/

CISCO OPEN SOURCE AND TECHNOLOGY VERIFICATION SERVICE
http://opensource.cisco.com/
http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/technology-verification.html

GOOGLE ANDROID OPEN SOURCE PROJECT AND CHROMIUM
https://source.android.com/
https://www.chromium.org/

MICROSOFT OPEN SOURCE AND GOVERNMENT SECURITY PROGRAM
https://opensource.microsoft.com/
https://www.microsoft.com/en-us/twc/government-security-program.aspx

ORACLE SOURCE CODE FOR OSS AND VIRTUALBOX
http://www.oracle.com/technetwork/opensource/index.html
https://www.virtualbox.org/wiki/Downloads

RED HAT OPEN SOURCE
https://www.redhat.com/de/open-source

VMWARE OPEN SOURCE
http://www.vmware.com/de/download/open_source.html

SCHRÖDINGER'S CAT

This is a thought experiment in physics that was proposed by Erwin Schrödinger in 1935. It directly transfers concepts of quantum mechanics to the macroscopic world in the form of a paradox. According to the thought experiment, the paradox is that a cat in a sealed box can, based on the rules of quantum mechanics, be in a state in which it is both 'dead' and 'alive' at the same time. The cat remains in this state until the box is opened and the cat is observed. The both dead and alive cat is only determined to be 'dead' or 'alive' when it is observed, i.e. when a measurement is taken.

DIGITAL SOCIETY

Information Security in the Quantum Age

By Dr Heike Hagemeier and Dr Manfred Lochter, section Requirements for and Development of Secure Cryptographic Mechanisms

‘For the past 30 years, we have expected the quantum computer to be a reality in about 10 years.’ This joke is still told, especially by those who are sceptical about the possibility of quantum computers. However, recent developments show that the time for action is now.

The security of digital infrastructures is nowadays largely based on public-key cryptography. The majority of systems used in the process are based on the presumed difficulty of certain mathematical problems. For example, the RSA cryptosystem is based on the fact that it is generally difficult to find the prime factors of large numbers.

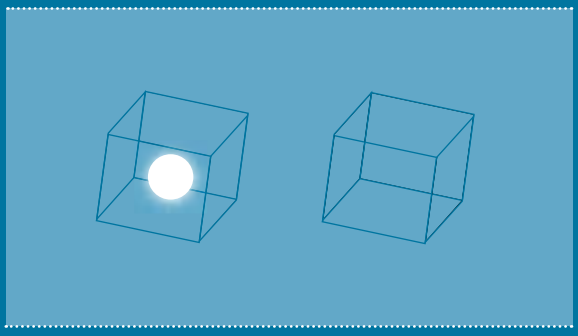
The tools available today mean that public-key systems cannot be broken when used correctly and with the correct key size.

However, as early as 1994 Peter Shor was shown an algorithm that would easily break these systems on what were then purely hypothetical quantum computers and would therefore remove the basis of today’s public-key cryptography. It should not be forgotten that Shor’s algorithm poses no threat to symmetrical systems (such as AES-256). In symmetrical systems, the key length required for potential attacks from a quantum computer would double (‘Grover’s algorithm’).

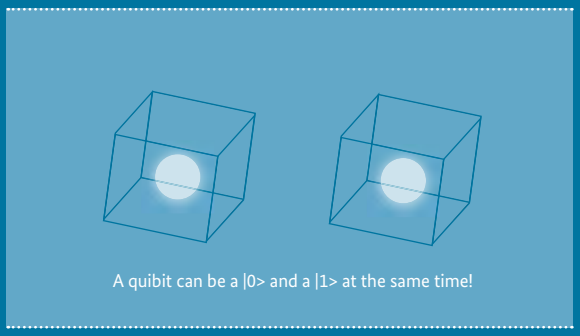
The idea of a quantum computer came from R. Feynman (at the start of the 1980s) and is based on the laws of quantum mechanics. A quantum computer would differ from the computers used today in that it would perform calculations using qubits rather than bits (see box).

A quantum computer capable of breaking cryptographic systems does not yet exist. However, significant progress has been made in developing the basic components required for this. The development of quantum computers has seen an explosion of interest in the research and industrial fields over the past few years. Global IT groups

BITS AND QUBITS



DEFINITION OF A BIT:
The state of a bit is 0 when the particle is in the left box, and the state is 1 when the particle is in the right box.



DEFINITION OF A QUBIT:
The state of a qubit is |0> when the quantum particle is in the left box, and the state is |1> when the quantum particle is in the right box.

Quantum computers use the principles of quantum physics. They make calculations using quantum bits (qubits), which – in contrast with standard bits – are able to simultaneously accept two states (with certain probabilities), which is referred to as superposition. A quantum computer can perform calculations with n entangled qubits in a single step, for which a traditional computer requires 2^n operations.

such as IBM, Google and Microsoft are investing substantial resources in quantum research and considerable progress has already been made. However, these companies are more interested in profitable applications of quantum computers, such as in the pharmaceutical industry or materials research. The EU is launching a flagship project, with one billion euros available to research quantum technologies and make them economically viable.

A QUANTUM LEAP FOR THE CRYPTOGRAPHY OF THE FUTURE

A new field of cryptography research has developed in parallel with advancing technology, namely post-quantum (PQ) cryptography. This concerns the development and investigation of cryptographic systems that cannot be broken by quantum computers. It should be noted in this context that these systems work on 'traditional' computers and therefore differ considerably from another current branch of research, quantum cryptography. Quantum cryptography attempts to use quantum mechanical effects for cryptographic applications. An example of this is quantum-based key distribution that exploits the properties of entangled particles.

The importance of post-quantum cryptography has increased markedly over the past few years: The NSA warned against quantum computers in August 2015 and initiated a migration to quantum computer-resistant systems. The NSA's justification for this is recent progress in physics and technology that could allow a cryptographically relevant quantum computer to be developed. The NSA did not mention any specific quantum computer-resistant systems, but referred to the future standards of the National Institute for Standards (NIST). The NIST has accordingly started work on the standardisation process for PQ cryptography.

Several international research groups are currently looking into the security and practicability of PQ cryptography. For example, the EU is now financing the European projects PQCrypto and SAFEcrypto as part of the Horizon 2020 programme.

Researchers are pursuing various approaches to developing quantum computer-resistant systems. These include, for example, grid-based systems, code-based systems and hash-based signatures. Hash-based Merkle signatures are thus far the only system that is generally considered to be

'The use of quantum computer-resistant systems will sooner or later become the standard for most cryptographic applications.'

safe and well-researched and is also recommended by the BSI (for example, for signing software updates). Grid-based systems also currently appear to be in more frequent use. For example, the grid-based algorithm 'New Hope' has been implemented on a trial basis on Google's Chrome browser as part of a key exchange. So far, however, research on many of the new systems is not practicable and has only been carried out to a limited extent. The standardisation of PQ cryptography is still in its infancy. Moreover, many of the security protocols used today also need to be adapted to PQ system formats. The migration to fundamentally new cryptographic systems is expected to be very slow and at times inefficient.

HOW MUCH TIME DO WE HAVE?

'I estimate a 1/7 chance of breaking RSA-2048 by 2026 and a 1/2 chance by 2031.'
Michele Mosca, Nov. 2015

Such estimates are naturally vague, but there is an acute need for action for cryptographic applications with long confidentiality periods. There is a risk that it will be possible to collect large volumes of encrypted data and decrypt it in the future using a quantum computer. The key agreement protocols used today also need to be secure for a suitably long period for the same reason.

In contrast, signatures that serve authentication purposes tend to have a rather short working life and in principle only have to be secure when they are verified. If it will be possible for a quantum computer to break a signature system in the future, then today's signature certificates are presumably already out of date. Caution only needs to be exercised if signature keys are valid for very long periods.

Sooner or later, the use of quantum computer-resistant systems will become the standard for most cryptographic applications. However, such use is not realistic in the near future due to the difficulties mentioned (e.g. practicability, compatibility). For the time being therefore, the BSI recommends the use of hybrid solutions wherever possible. 'Hybrid' in this context means a combination of traditional systems and suitable quantum computer-resistant solutions. A huge variety of approaches is conceivable here.

Moreover, the new and further development of applications should ensure that they are designed as flexibly as possible in order to respond to all conceivable developments, to implement future recommendations and standards and to replace algorithms which may be weaker in the future. ■

Profile in brief:

Professor Michael Meier heads the Cyber Security Department at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE). This department analyses attack techniques and develops monitoring processes and control mechanisms to protect against cyber attacks on IT systems.
Professor Meier holds the chair for IT security at the Institute for Informatics at the University of Bonn, in collaboration with the FKIE. His research work focuses on applied aspects of IT security, attack and malware analyses.

NETWORKING WITH SIDE EFFECTS

By Prof. Michael Meier, Head of the Cyber Security department at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE)

Security and the Internet of Things

The Internet of Things (IoT) makes life smarter in many households. Cameras, baby monitors, televisions and thermostats in smart homes are connected to the Internet – and need to be protected against cyber attacks.

The security properties of most IoT systems are anything but smart. Standard passwords are often used which, once hacked, grant access to all devices of the same type. For cost reasons, many manufacturers also manage without update strategies, which can regularly close vulnerabilities in the device software. Cyber criminals exploit these weaknesses. They bring as many internet-capable devices as possible under their control so that they can misuse them for their own purposes – a method that caused a furore in October last year in the case of the Mirai botnet. The operators of this large network control more than 400,000 IT components in order to carry out denial-of-service (DoS) attacks: They overload the servers of popular internet services and therefore force them to crash.

Prof. Jürgen Beyerer, Institute Director of the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB), and the Federal Minister for Education and Research, Prof. Johanna Wanka, at the opening of the 'Cyber Security' learning laboratory in Görlitz.

THE DUTY OF MANUFACTURERS AND USERS

As these attacks cause massive economic damage, IoT devices need to be protected against them. On one hand, the sale of the systems must go hand in hand with binding security standards, standard passwords must be prohibited and security updates must be provided regularly. On the other hand however, users should also be required to play their part in protecting their internet-capable devices. Even if they are not legally liable for cyber attacks, it is however negligent not to reset the router password, for example, when the media reports that the devices are targeted by the Mirai botnet. Just like when they take medication, users need to be informed that IoT networking has 'side effects'. If they don't protect their IT.

CYBER SECURITY IS A QUESTION OF QUALIFICATION

Ultimately, however, security measures must also be integrated into the device design so that they are easy for users to implement. The responsible employees need to be trained for this. The Fraunhofer Academy, the continuing education establishment of the Fraunhofer Society, develops various training routes and modules, some of which focus explicitly on IoT security, for its 'Cyber Security' learning laboratory. The career-compatible continuing education format imparts the latest expertise from cutting-edge research and enables employees – from security experts to developers and management – to make IoT devices secure. ■

IoT – of course!

By Arne Schönbohm, President of the BSI

The cyber attack on the Internet Service Provider Dyn clearly showed in October 2016 that digitalisation cannot be successful without cyber security. Attackers search the Internet for vulnerable network devices, find what they are looking for hundreds of thousands of times over, and bring these devices together to form a powerful botnet. This doesn't just affect computers, laptops and mobile devices, but also household devices which are increasingly connected to the Internet as part of the Internet of Things (IoT). Users often don't notice that their devices have been taken over.

The BSI shapes IT security by means of prevention, detection and response, and therefore calls for IoT manufacturers to consider not only functional and pricing elements in product development, but also the following security requirements:

- Users should be able to change pre-set access data and passwords for all device access options (e.g. via HTTP, TELNET or SSH).
- If passwords cannot be personalised, IoT devices should force their users to change passwords before the devices are used for the first time.
- It should be possible to deactivate unused services.
- The IoT device's incoming and outgoing communication should only be sent using cryptographically protected protocols such as TLS.
- IoT devices must not automatically produce an unsecure configuration in the router via Universal Plug and Play (UPnP), thereby allowing connections to unsecure services.
- To impede cyber attacks in the longer term, manufacturers should undertake to provide security updates regularly that can be transferred and installed in a cryptographically protected format.
- Product firmware should also be sufficiently hardened, thereby, for example, preventing the downloading of content from the Internet.

The BSI will intensify its dialogue with manufacturers and associations to develop joint solutions.

Smart Meter Gateway

By Dennis Laupichler, head of section Cyber Security for Digitalisation of the Energy Transition

Cyber Security for the Digitalisation of the Energy Transformation

Smart metering systems are important components in the smart network and need 'Security & Privacy by Design'. As the central communication platform of the smart metering system, the smart meter gateway allows secure implementation in a wide range of applications and is the driver of innovation in digitalisation. In conjunction with the BSI's technical standards, the law on digitalising the energy revolution will create a binding framework for the secure and privacy-compliant use of smart metering systems in various fields of application. The drafting of mandatory minimum requirements for the secure integration of vehicle charging stations into the smart network will now follow.

DIGITAL TRANSFORMATION OF THE ENERGY INDUSTRY

The digitalisation of all aspects of company life, associated with the boom in technology, is creating major challenges for governments, the economy and our society. Within the energy industry, both the digital transformation of the energy system, and the integration of decentralised and renewable energy plants are radically transforming the supply chain. New, innovative business models are emerging, and companies that were not previously involved in the sector are now active in the German energy market as new competitors.

This increasing digitalisation and networking in the energy industry are leading to improved efficiency and process optimisations, as well as greater convenience due to the communication between product components and systems. On the other hand, future growth in digitalisation and networking also means a significant rise in potential threats. This is because the number of vulnerabilities is increasing, communications infrastructures are becoming more and more complex and the data volumes being processed are growing.

The likelihood of successful attacks on digitalised infrastructures is therefore becoming greater. This means that having demonstrably secure product components and systems in the network, as well as a secure communications infrastructure, are now critical in retaining user trust.

DATA PROTECTION AND DATA SECURITY

Successful digital transformation can only be achieved through early development and provision of generally binding safety standards and measures to ensure that digital infrastructures are trustworthy. Electronic identities and encryption play a central role here by ensuring that digitalisation is secure and complies with data protection requirements. In this regard, new technologies must not only be developed in Germany, but must also be successfully integrated in order for them to play a leading management role within future digital markets and, ultimately, to achieve energy transformation as a company objective as part of the shift to digital.

BSI LEGAL FRAMEWORK AND TECHNICAL STANDARDS

The law on digitalising energy transformation, which came into force on 2 September 2016, takes account of these key requirements and therefore establishes critical requirements for setting up an intelligent infrastructure for energy transformation. The issues covered by Article 1 of the new Smart Meter Operation Law (MsbG, Article 1 Law on the digitalisation of the energy transition) include defining higher

'In the future, integrating the smart meter gateway into charging stations will enable secure charging that complies with data protection requirements and will also allow vehicle charging to be billed.'

technical standards for smart metering systems in the form of protection profiles (PP) and technical guidelines by BSI to ensure data protection, data security and interoperability.

THE GOVERNMENT AND ECONOMY ARE WORKING TOWARDS MUTUAL SECURITY STANDARDS

Establishing binding framework provisions for the production and operation of smart metering systems is key to establishing trust in and acceptance of the new technologies, particularly since the technologies process personal data. On behalf of the Federal Ministry for Economic Affairs and Energy, the BSI has therefore developed requirements for trustworthy product components (smart meter gateway with integrated safety module) and their safe IT operation (administration), and for a trustworthy communications infrastructure (smart metering public key infrastructure).

These developments involved various organisations within telecommunications, information technology, energy, housing and consumer protection, as well as Federal Commissioner for Data Protection and Freedom of Information (BfDI), the Federal Network Agency and the Federal Physical-Technical Institute.

The law on digitalising the energy revolution allows continual, gradual upgrades to the smart metering system and other components to enable other applications. These include managing the supply and load of producers and users to benefit the grid, integrating further business lines (gas, water, heating), and developing vehicle charging station infrastructure within the electromobility sector.

SECURE INTEGRATION OF CHARGING STATION INFRASTRUCTURE FOR ELECTRIC VEHICLES

Pursuant to section 48 MsbG, the legal framework already sets out, in perspective, the binding minimum requirements for secure integration of electric vehicle charging station infrastructure into the smart grid. The use of electric vehicle batteries as power storage and the production of control energy, both of which offset fluctuating supply from wind farms and photovoltaic plants, will play a vital role in the future.

At the same time, electric vehicle charging processes must be aligned in advance within energy management systems to prevent grid fluctuations and negative feedback in the smart grid. In future, integrating the smart meter gateway into charging stations will allow secure charging that is compliant with data privacy requirements and will allow vehicle charging to be billed. In addition to the requirements for charging stations and the overall system architecture, other critical elements include secure authentication procedures, secure administration and operation of charging points, metered values processed in accordance with data protection requirements, and the need for a trustworthy communications infrastructure.

BSI will work with the Federal Ministry for Economic Affairs and Energy to initiate dialogue and agreements with organisations, interest groups and funding projects to securely integrate electric vehicle charging station infrastructure into the smart power grid. ■

For more information see www.bsi.bund.de/SmartMeter

Since the US presidential elections, everyone has been talking about them: socialbots. Socialbots mainly work their mischief on social media such as Facebook and Twitter. They are computer programs that, once activated, automatically replicate on the Internet without any further human intervention. The aim of socialbots is to create a particular perception that portrays a supposed social reality. They do this through sheer mass of posts such as Tweets, Retweets, comments and Likes. Experts are unanimous: this technology can be successfully used to influence political discussion and can ultimately be damaging to democracy.

SOCIALBOTS

Bot Battles for Online Opinion Leadership

After Donald Trump's success in the US presidential race, most observers have no doubt: Never before have social media had such a strong bearing on the outcome of a political election as in the USA in autumn 2016. What is more, it is only a few years since social media became ubiquitous in our increasingly digital, connected society. Now, almost one in three Germans use social media according to the Reuters Institute Digital News report in July 2016, and not just as a way to stay in touch with acquaintances but also as news sources alongside newspapers and television. Against this backdrop, the increasingly widespread use of socialbots is particularly significant.

FIFTY YEARS OF CHATBOTS

Automated dialogue systems like socialbots and chatbots had already emerged in the 1960s, when computer scientist Joseph Weizenbaum developed the computer-based language processing program ELIZA, which was an ingenious early application of artificial intelligence. The technological revolution of recent years has resulted in significant advances in data processing, as well as in the development of artificial intelligence. The obstacles to development and to using socialbots have therefore all but disappeared. It is comparatively straightforward and cost-effective to write programs that can be deployed within social networks to like, recommend and comment on other comments and on posts.

Advanced versions can even create user profiles independently, complete with photograph, name and other information. There are also more complex forms of the bots programmed with artificial intelligence, and these are already capable of writing longer text and exchanging ideas. The crux of the matter is that: a normal internet user is not able to distinguish between one of these bot profiles or posts and those of a real human. Socialbots connect with other fake users as well as genuine ones; they comment on news, share and like posts, and achieve a level of activity that a genuine internet user could hardly achieve in real life. Meanwhile, the opinion leadership of these active, connected 'opinion robots' is provided by social network algorithms. The more often content is clicked on or shared, the more prominent its position on the platforms; this means that those who already have a large number of followers will reach all the more new users. On this basis, the effect of just a few bots and users can be very substantial. This opens the door wide to the manipulation of public opinion.

ARTIFICIAL INFLUENCE ON FEDERAL ELECTIONS?

With election day fast approaching, threats related to socialbots have climbed right to the top of the agenda. Federal Minister of the Interior Thomas de Maizière recently stated that he would 'advocate for a public declaration by all the parties in Germany taking part in the Federal elections that they will not participate in such activities.'

BSI is keeping a very close watch on the developments in this area. As discussed in the current IT situation report, BSI has already discovered attacks against parties, media and public institutions, fuelling concerns that third parties will attempt to manipulate public opinion. This includes the effects of activities carried out by 'trolls'. Unlike socialbots, trolls conceal real humans who are paid to spread targeted disinformation campaigns and false reports, or fake news, in order to influence public opinion. Given that social media is fast, and that once something is online it becomes global, it is extremely difficult to remove fake news again or persuade people to forget about it. ■

AND FINALLY

EVENTS CALENDAR 2017

15th German IT Security Conference

16th - 18th May 2017 in Bonn-Bad Godesberg

The digitalisation and networking of many areas of life and work is gathering pace. At the same time, technical innovations in areas such as Industry 4.0 and intelligent traffic systems or in the context of the energy revolution are making it clear that the potential uses of information technology are far from exhausted. These developments can, however, only be successfully implemented if aspects of IT security are given due consideration alongside functionality and financial factors. Digitalisation without IT security will ultimately not work.

In light of the rapid speed of innovation and the resulting economic success, the security of IT products is rarely accorded equal importance by either users or providers. The specific challenge here is to reconcile security goals with user demands and to develop products which meet the requirements of the users.

One approach is to start now with creating standards for current developments in fields such as the automotive industry, Industry 4.0 or mobile applications which would incorporate established procedures and knowledge into product development. And last but not least, user protection, i.e. the protection of citizens using digital communication and services, plays an important role in this. Whether for business, government or society, the same applies. All of them have to find a balance between too much security and too much risk tolerance.

For this reason, the 15th German IT Security Conference is called:

'Digital Society Between Risk Tolerance and Security Requirements'

With more than 600 visiting experts (in 2015), the German IT Security Conference organised bi-annually by the BSI is a fixture in the IT security industry calendar. Attendees will discuss the status of national and international IT security developments over three days. The conference aims to highlight the topic of IT security from different perspectives, and to present and develop solutions. An accompanying exhibition complements the lecture program.

Information on attendance options, and the lecture programme and accompanying exhibition at:
https://www.bsi.bund.de/IT-Sicherheitskongress

OTHER EVENTS WITH BSI INVOLVEMENT:

Hannover Messe Industrie (HMI)

24th–28th April 2017

The BSI will be represented with its own stand (Hall 8, Stand D29) at the Hanover Industry Trade Fair (HMI) from 24th to 28th April 2017 and will be offering information on current requirements of cyber security and IT security projects related to the industry. The BSI will be presenting a wide range of expert opinions on secure digitalisation for government, business and society.

konaktiva job fair

9th - 11th May 2017

ITS.connect job fair

19th May 2017

The BSI will be presenting itself as a potential employer at the konaktiva job fair at the Technica University of Darmstadt and the ITS.connect job fair in Bochum. Interested students and graduates will receive information on career entry, opportunities and the exciting prospects available to the BSI employees.

it-sa

10th–12th October 2017

From 10th to 12th October 2017, the BSI will have its own stand and give various presentations at the it-sa in Nuremberg. Together with the Federal Association for Information Management, Telecommunications and New Media (BITKOM e.V.), the BSI will be acting as a promotional supporter.

it-sa is the only IT security fair in the German-speaking countries and one of the most important worldwide. Whether cloud computing, IT forensics, data security or hosting, the fair is a unique platform for IT security officers, developers and providers of IT security products and services.

A current preview of the events which the BSI will attend can be found at:
https://www.bsi.bund.de/Veranstaltungen

We want your digital perspective

Photos © iStock.com/Grafissimo; © iStock.com/Krasyuk

Federal Office
for Information Security

Information technology forms the foundation of modern life, making it all the more important for people to be able to trust the digital world; this is what we take care of. We are the national authority for cyber security, shaping IT security in Germany as well as in Europe and worldwide, working together with the worlds of commerce and science. We advise political and administrative bodies and are in dialogue with the public as well as a multitude of associations. Our experts are valued and sought-after in international discussion, and we do all this with one shared goal: information security. We ensure that the future will be able to grow from the network. With around 650 employees, we are a comparatively small team, but with huge responsibility – and that's why we need you with us.

For more information see www.bsi.bund.de/karriere and bewerbung@bsi.bund.de or phone +49 (0)228 99 9582 0

LEGAL NOTICE

Published by:	Federal Office for Information Security (BSI) 53175 Bonn, Germany
Source:	Federal Office for Information Security (BSI) Section B23 – Cyber Security for Citizens and Public Relations Godesberger Allee 185–189 53175 Bonn, Germany Telephone: +49 (0) 22899 9582-0 E-Mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Last updated:	March 2017
Texte und Redaktion:	Stephan Kohzer und Nora Basting, Federal Office for Information Security (BSI) Joachim Gutmann, GLC Glücksburg Consulting AG Fink & Fuchs AG
Concept, editing and design:	Fink & Fuchs AG Berliner Straße 164 65205 Wiesbaden Internet: www.finkfuchs.de
Printed by:	Druck- und Verlagshaus Zarbock GmbH & Co KG Sontraer Str. 6 60386 Frankfurt a.M. Internet: www.zarbock.de
Item number:	BSI-Mag 17/705-1e
Image credits:	Title: Henning Schacht (picture), BSI (background); p. 1: Stephan Kohzer/BSI; p. 4 Catharina Frank (top left), Sabrina Löhr, Posteo e.K. (middle), Stephan Kohzer/BSI (below right); p. 5 CSCG, Institut für Internet-Sicherheit – if(is) (top left); p. 6–7: R. Winkler; p. 8: MeinUnternehmensfilm GmbH; p. 10: R. Winkler; p. 11 Henning Schacht; p. 12: Karin Berneburg/BILDSCHÖN GmbH; p. 13: Karin Berneburg/BILDSCHÖN GmbH; p. 14: bluedesign/fotolia; p. 16: liuzishan/fotolia; p. 19: Henning Schacht; p. 20: kasto/fotolia (top left), Henning Schacht (top right); p. 21: Henning Schacht (top left), Henning Schacht (top right); p. 22–23: R. Winkler; p. 24: Deutsche Cyber-Sicherheitsorganisation GmbH; p. 25: R. Winkler; p. 27: Stephan Kohzer/BSI; p. 28–29: R. Winkler; p. 30-31: Stephan Kohzer/BSI; p. 32: R. Winkler; p. 34: Stephan Kohzer/BSI; p. 35: Stephan Kohzer/BSI (top left), Fink & Fuchs AG, Fotos iStock.com/Grafissimo, iStock.com/Krasyuk (above left.); p. 36: Henning Schacht; p. 38: Leo Leowald; p. 39: Leo Leowald; p. 41: BSI; S. 42: R. Winkler; p. 44: Deutschland sicher im Netz e.V.;p. 46–47: enanuchit/fotolia; p. 48: dstarky/fotolia (picture), ICS Security in Maritime Transportation U.S. Department of Transportation (concept); p. 49: R. Winkler; p. 51: BSI; p. 52: R. Winkler; p. 54: R. Winkler; p. 56: R. Winkler; p. 58: nexusplexus/123 RF Lizenzfreie Bilder (background), Fraunhofer (top left); p. 59: Fraunhofer (top left), Stephan Kohzer/BSI (above left); p. 61: Björn Wylezich/fotolia; p. 62: R. Winkler, Herrndorff/fotolia (hand); p. 64–65: Kwangmoo/fotolia; p. 66: Fink & Fuchs AG, Fotos iStock.com/Grafissimo; iStock.com/Krasyuk

The BSI Magazine is published bi-annually. 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.

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

www.bsi.bund.de