Federal Office
for Information Security

BSI Magazine 2018/01

Security in focus

Industrial Control Systems in Industry 4.0

BSI INTERNATIONAL

National Cyber Security Centre (NCSC)

SPECIAL FEATURE

Cyber Security in Industry 4.0

DIGITAL SOCIETY

Blockchains in Use

EDITORIAL

Sustainable Security Awareness

Modern industrial plants today are highly interconnected systems. Many companies – from SMEs to industrial groups – are increasingly valuing the exchange of information with suppliers or customers as quickly and directly as possible. To achieve this, areas that were previously physically separated from each other are be connected over the Internet – and can therefore be attacked. Cyber criminals can exploit these attack surfaces. Sabotage, espionage and blackmail are often the consequences.

Attacks on industrial plants, sometimes with serious consequences, have been observed time and again in recent years. Industrial control systems, which play a central role in production safety and are therefore particularly crucial to protect, are especially threatened. Against this backdrop, companies have become more aware of Cyber Security – and not merely in the critical infrastructures IT Security law obliges them to invest in for the Cyber Security of their systems.

“Only when security aspects are initially considered in the design, can digitalisation succeed .”

Cyber Security plays a key role in the digitalisation of production processes. Only when security aspects are initially considered in the design, can digitalisation succeed in developing the desired potential for companies. An important concern of the BSI is therefore to foster sustainable security awareness among business and to lay a solid foundation for digitalisation.

What threat do attacks on industrial control systems pose? How can companies create the adequate conditions to protect themselves? How can Security by Design help to meet the growing challenges? In the latest issue of the BSI Magazine, we present some aspects of cyber security in the world of Industrie 4.0. We hope you enjoy reading it!

Sincerely Yours,

Arne Schönbohm,
President of the Federal Office for Information Security

TABLE OF CONTENTS

NEWS

4 In Brief

BSI INTERNATIONAL

6 National Cyber Security Centre (NCSC) – Interview with Ciaran Martin
10 International Symposium ViS!T at the it-sa for the First Time
12 Regulation for Digital Services

CYBER SECURITY

14 Getting Started – Made Easy: Basic Protection according to IT Grundschutz
16 Cyber-Safe Driving – Automated and Connected Vehicles
18 Security for Developers – Technical Guideline for Cryptography
22 Contact Point and Exchange Platform – Alliance for Cyber Security

SPECIAL FEATURE

24 Industry 4.0 – Security by Design
26 Joint Responsibility
28 Cyber Threats for Industrial Plants
30 Security for Safety – No Hype, But Necessity
32 Secure Identities: Necessary Starting Point for Business Processes – Interview with Michael Jochem

THE BSI

34 Advantage Diversity
36 Expanding the Cooperation with Federal States

IT SECURITY IN PRACTICE

40 Avalanche Sinkholing – Many Systems are still Infected
42 Putting IT Security into Action
44 Lukas Hospital: Armed against Cyber Attacks

DIGITAL SOCIETY

48 Blockchains in Use
52 Data Security for Connected Mobility
53 Basic Tip from the BSI – Smart Home
54 Consumers in the Digital World

AND FINALLY

56 Events 2018/19
58 Subscription Order Page
59 Legal Notice

NEWS

Report on the State of IT Security 2017

Report on the State of IT Security 2017 Presented in Berlin

On 8 November 2017 in Berlin, the former Federal Minister of the Interior Thomas de Maizière and the President of the BSI Arne Schönbohm presented the BSI's report on the state of IT Security in Germany in 2017. The National Cyber Security Authority's annual status report details and analyses the current status of IT Security, the causes of cyber-attacks and the methods and means behind those attacks. This process allows the BSI to present solutions for improving IT Security in Germany.

The threat situation remained severe, at a high level throughout the reporting period of July 2016 to June 2017. Traditional cyber-attack entry gates remained critical. An increase in IT Security incidents involving ransomware indicated above all where cyber criminals have found a lucrative opportunity to extort large sums of money.

For more information see https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

SPS Drives

SPS IPC Drives 2017

The Federal Office for Information Security (BSI) was on exhibit at SPS IPC Drives 2017 in Nuremberg. The international trade fair for electrical automation provided a platform for the BSI to inform the interested public about the challenges of digitalisation that particularly arise in conjunction with industrial security and "Industry 4.0."

For more information see
https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_SPSIPCDrives_27112017.html

Award

Successful BSI Personnel Campaign

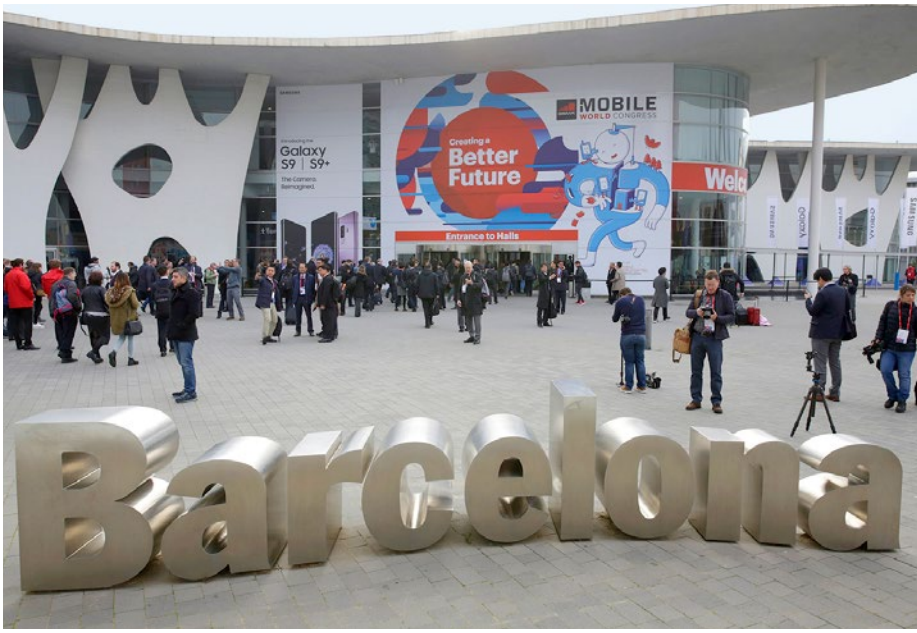
The BSI launched a personnel marketing offensive to fill 180 newly created positions last year. The advertising campaign designed to support it seems to have been very well received by its target audience: readers of the student magazine "audimax" voted it their favourite of issue 5/17. The BSI will continue recruiting new employees in 2018 under the motto "We want your digital perspective"

For more information see https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news_erfolgreiche_Mitarbeiterwerbung_23012018.html

Exhibition

Mobile World Congress 2018

The Federal Office for Information Security (BSI) was an exhibitor at the Mobile World Congress, Europe's largest mobile phone trade fair, for the first time from 26 February to 1 March 2018 in Barcelona. The National Cyber Security Authority presented solutions for tightening mobile application security with secure identification and authentication at its booth shared with the state of North Rhine-Westphalia in Hall 6, Booth 6B40.



For more information see https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Mobile_World_23022018.html

BSI INTERNATIONAL

NATIONAL CYBER SECURITY CENTRE (NCSC)

The National Cyber Security Centre Headquarter in London

„The Core of NCSC Mission: Communicating with the Public."

Interview mit Ciaran Martin, CEO NCSC

The UK's National Cyber Security Centre (NCSC) was launched in 2016 as part of GCHQ (Government Communications Headquarters) and provides the UK with a single, central body for Cyber Security at a national level. We are here to do four main things – first and foremost to manage the response to incidents, and then to protect Critical Infrastructure. We also want to make sure that people are able to protect themselves automatically, and to make the Internet a safer place to be. Through all of this, we want to work with our international friends.

NCSC has been launched about one and a half year ago. What has been the main goal of founding NCSC UK as a part GCHQ?

The UK Government is really serious about Cyber Security. It felt that the current strategy had run its course and that there were too many institutions working on it, but without anyone owning the problem. This is why in 2015 we decided to change strategy and to reorganise. Changing strategy meant focusing on what the government could do to thwart criminal, but unsophisticated, attacks: that's where our Active Cyber Defence programme came in. We could have set up the NCSC outside the intelligence community, but it was felt that GCHQ had access to data capabilities, skills and partnerships that nobody else had and couldn't be replicated in a new organisation. So we founded the NCSC as a part of GCHQ, on the condition that the NCSC did some things differently from the rest of GCHQ – in particular what is absolutely core to its mission: communicating with the public.

„The Active Cyber Defense program has reduced the average online time of a phishing site from 27 to one hour.“

What have been successes of NCSC UK since its creation?

The reality of the threat we face – large, growing and diverse – means that some attacks will get through, and the first duty of the NCSC is to help manage and mitigate the impact of those attacks. In our first year of operations we responded to 590 significant attacks, ranging from attacks on key national institutions like the National Health Service (NHS) and the UK and Scottish Parliaments, through to attacks on large and small businesses and other organisations.

We launched our world-leading Active Cyber Defence programme in 2017, preventing thousands of attacks and redu-cing the average time a phishing site is online from 27 hours to 1 hour. Through CyberFirst we are helping to nurture the next generation of cyber experts by hosting more than 1,000 young people on courses, while last year 8,000 young women were inspired to enter our inaugural CyberFirst Girls Competition.

We've also created the pioneering Industry 100 initiative to work with or embed 100 industry professionals within the NCSC, and globally we have worked with more than 50 countries across 5 continents, including signing a ground-breaking Memorandum of Understanding with NATO.

Where do you see potential for future development and improvement of NCSC UK?

We are proud of what we achieved in our first year, but there is so much more to do in our second year, and the years ahead, to counter this strategic threat to our values, prosperity and way of life.

We need to keep working together with academia and industry to ensure we understand private sector demand for cyber security skills - both now and in future - and to ensure we have the capability to fill that gap.

We also need to get to a stage where organisations are able to achieve a sufficient level of cyber defence independently, leaving us with greater capacity to focus on the state threats that only government can deal with.

Lack of diversity is a huge problem within the cyber security industry and one that the NCSC is trying to combat through initiatives such as the CyberFirst Girls Competition, but there is still a lot of work to do. A diverse set of problems requires a diverse set of people. Only 1 in 10 people working in the industry is female, and at the NCSC that figure rises to a third – but that's still not good enough and it's something we want and need to fix.

What is the feedback NCSC UK gets from its target groups?

The feedback has been overwhelmingly positive across the target groups of the NCSC's different directorates.

94% of delegates to the NCSC's flagship conference 'CYBERUK' said that they had increased their understanding of why the NCSC has been created, our structure, approach and its role in the implementation of the National Cyber Security Strategy.

Since the launch of the Cyber Information Sharing Partnership (CiSP) - our online communications forum - in March 2013, the value of this collaboration has been recognised by industry, with membership growing considerably (by 43% in the last year). As of December 2017, over 4,020 organisations and 9,097 individuals have signed up from across 30 different sectors. CiSP was invaluable during the WannaCry ransomware attack, providing up-to-the-minute mitigation advice whilst also debunking false rumours.

Many of the entrants of our CyberFirst Girls Competition are now expressing interest in pursuing careers in computer science.

With over 100,000 visitors to the NCSC website in a single month, our website is becoming a cornerstone of the cyber community. Our twitter account has over 32,000 followers who engage constructively with the advice that we post there.

Profile in brief:

Ciaran Martin was announced as the first CEO of the NCSC on 15 March 2016, having been GCHQ's Director General for Cyber Security since February 2014. Until April 2016 he was also responsible for GCHQ's strategy for managing information risk and has led on policy and communications for the department.

Which are your strategic topics in Cyber Security for the next years? Nationally and Internationally?

The most important thing we can do is raise basic defences – I think we have figured out some ways of doing that and we need to do them at the right scale. Second is making technology much safer automatically, including building security into design. A third priority is keeping our most sophisticated capabilities up to scratch so we can tackle the most sophisticated actors. A final point is doing all the above at an international scale with our allies and friends. I strongly believe that the Internet did not invent liberal western values: it was invented by them and these freedoms are precious and hard won. Countries like the UK and Germany are on the same side in defending them.

How is your assessment about the cooperation of NCSC UK with Germany and BSI?

Germany is one of the NCSC's most important partnerships. Arne Schönbohm and I meet regularly to discuss the common challenges we face and our cooperation with BSI, especially on incident response, is extremely valuable. I was really disappointed that I had to pull out of addressing the BSI's congress last May at short notice, however it was right in the middle of the WannaCry crisis so Arne Schönbohm was very understanding!

Have you identified common topics of interest with Germany, where do you see differences?

We have far more in common with Germany than differences: when I look across the portfolio of both of our work on cyber I see very little in it that could only be the focus of a UK-based or German company.

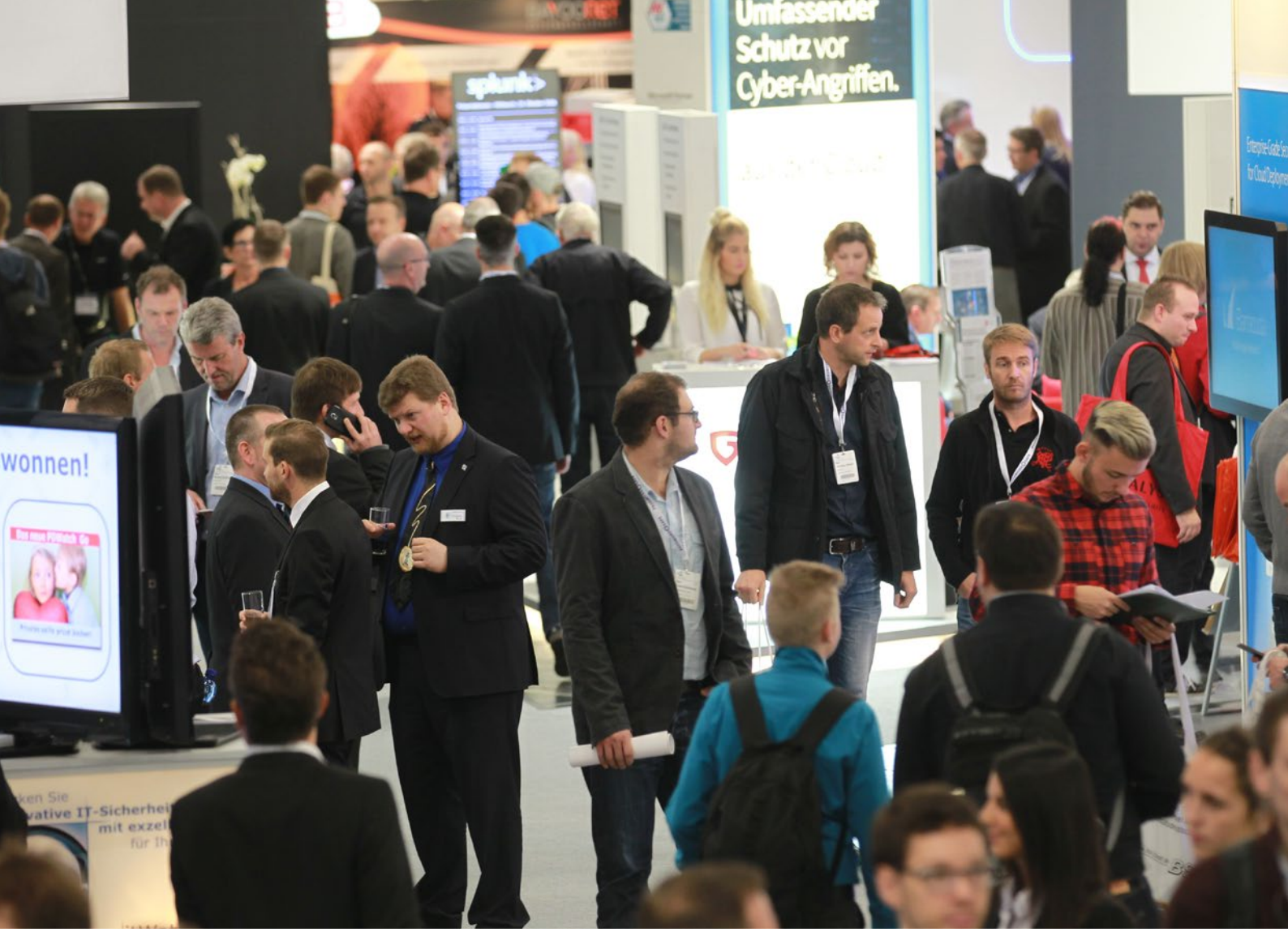
How is NCSC UK going to handle the challenges coming with Brexit?

We don't know yet what exact form the UK's future relationship with the EU will take. But from the very start, the Government has said that it wants a deep and special partnership with the EU. On security, we have said our commitment to Europe is unconditional so whatever happens we want to be a close partner with Germany on Cyber Security.

Next year GCHQ is going to celebrate its 100th anniversary. What do you think... What will the historians see when they look back on the history of NCSC UK and the history of Cyber Security, when NCSC celebrates its 100th anniversary 2116?

All of us involved in the early days of the NCSC are really excited about it, and I hope that this will be remembered as a time we did something special and innovative with a government agency. It is not often that you are given the chance to take a new approach and solve a problem from scratch, and to do this all with partners. What we do now in Cyber Security will determine how free, safe and pros-perous we are for the next century, so I want historians to look back and see the NCSC as the cornerstone of those values.

For more information see https://www.ncsc.gov.uk/



International Symposium ViS!T at the it-sa for the First Time

Secure Information Technology in Administration

For the first time, the symposium “Administration Integrates Secure Information Technology” – or ViS!T – will be held in Nuremberg at the IT Security trade fair it-sa. At the invitation of the BSI, experts from Germany, Austria, Switzerland and Luxembourg will discuss a range of current challenges in the secure design of IT processes. The symposium takes place every two years and is organised alternately by one of the participating countries.

The ViS!T symposium is aimed at employees in public administration in the participating countries. The target audience is not necessarily only IT specialists. The symposium also and above all addresses generalists and strategists. It deals with the exchange of experiences, the multilateral discussion about projects with a focus on IT Security.

Besides the BSI from Germany, the Centre for Secure Information Technology – Austria (A-Sit) from Austria, the IT management body of the Swiss Confederation FSUIT and the government of the Grand Duchy of Luxembourg are involved. The parties aim to achieve a comparable and, if possible, binding IT Security level in the participating countries.

This year's ViS!T symposium will take place on 8-9 October at the it-sa IT Security trade fair, which will open its doors in Nuremberg from 9-11 October. The ViS!T programme, which will take place for the ninth time this year, discussions are taking place on IT Security issues in administration. This includes topics such as blockchain, IT/information security laws and digitalisation. About one hundred participants are expected. If you would also like to take part, you can register quickly at https://www.bsi.bund.de/anmeldung_visit.

With 630 exhibitors from 24 countries and more than 12,000 trade fair visitors last year, it-sa is one of the most important trade fairs for IT Security worldwide. Since 2009, it has been an independent trade fair for anyone interested in the subject of IT Security on a professional level. That includes developers and practitioners as well as project managers and executives. This year, the network of partners at it-sa will be expanded to include Sicherheitsnetzwerk München (Security Network Munich) and the Information Security Society Switzerland (ISSS). ■

Symposium ViS!T: PARTICIPATING INSTITUTIONS

Federal Office for Information Security

The **Federal Office for Information Security (BSI)** was founded in 1991 and is a higher federal authority under the Federal Ministry of the Interior. As the National Cyber Security Authority, the BSI designs information security in digitalisation through prevention, detection and reaction for government, the business world and society.

A-SIT

The **Secure Information Technology Centre Austria (A-SIT)** was founded in 1999 as a registered non-profit association and has established itself as a competence centre for IT Security. Its members are the public institutions Federal Ministry for Digital and Economic Affairs (BMDW), Central Bank of the Republic of Austria (OeNB), Graz University of Technology (TU Graz) and the Federal Computing Centre (BRZ).

The **Federal IT Steering Unit (FITSU)** ensures implementation of the information and communication technologies (ICT) strategy in the Federal Administration of Switzerland. For this purpose, it issues guidelines for administrative units and manages ICT standard services. FITSU also manages the eGovernment Switzerland Programme Office as well as the Reporting and Analysis Centre for Information Assurance (MELANI).

On 21 January 2015, the **government of the Grand Duchy of Luxembourg** adopted the draft decree for setting governance on information security management, which includes the creation of a National Information System Security Agency (ANSSI) for the public sector and Critical Infrastructures.

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

Regulation for Digital Services

By Marc Schober, Head of Section Critical Infrastructure Sectors: Financial Services and Insurance, IT and Telecommunications, Digital Service

New Rules as of Mai 2018

New rules for a Europe-wide consistent minimum-security level strengthen the protection of online marketplaces, search engines and cloud services. Furthermore, the newly introduced obligation to report "Security incidents with significant impact" improves the coordinated response to cyber-attacks. Digital service providers must comply with the requirements by May 2018.

Supplying the business world and society with electricity, telecommunications and other critical services without interruption has always been essential. Organisations, institutions and companies that guarantee this are known as Critical Infrastructure Providers whose Critical Infrastructures require special protection against cyber-attacks. This was consequently ensured with the IT Security Act of 2015 and the EU Directive on Network and Information Security (NIS Directive) adopted in 2016.

But as a result of constantly accelerating digitalisation, the dependence of business and society goes far beyond the realm of Critical Infrastructures. Digital services such as search engines, cloud services and online marketplaces must also function without disruption and provide their users with an appropriate level of security. The NIS Directive therefore provides, in addition to the regulation of Critical Infrastructures, EU-wide harmonised regulation of digital service providers. The regulations were written into national law with the act for the implementation of the NIS Directive in the summer of 2017 (Section 8c BSIG) and will be applicable as of 10 May 2018.

DIGITAL SERVICES

Digital services in the legal context are exclusively online marketplaces, online search engines and cloud computing services (Section 2 (11) BSIG). Social networks and map and navigation applications are not covered by the regulations.

- **Online marketplaces within the meaning of the law must bundle offers of several providers and make contract conclusion possible. Online shops of individual retailers or pure price comparison portals are therefore not covered by the new regulation.**
- **Search functions limited to own web offers expressly do not apply as online search engines.**
- **Cloud computing services must provide access to a scalable and resilient pool of shared computing resources within the meaning of the law.**

In contrast to the Critical Infrastructure regulation, all providers from affected service categories are automatically subject to regulation unless being considered as micro or small enterprises, having fewer than 50 employees or generate less than EUR 10 million in annual sales.

The EU member state responsible for overseeing the provider depends on the provider's headquarters. If this is outside the EU, the location of a representative nominated by the provider has jurisdiction. Some large providers are therefore not under the responsibility of the BSI, despite the German market playing a central role in their European activity. This disadvantage is offset by closer networking between national authorities and the Member States' Computer Security Incident Response Teams (CSIRTs).

TECHNICAL UND ORGANISATIONAL MEASURES

The new regulations focus on the objective of preventing security incidents or minimizing their impact on digital services. For this purpose, the providers have to take the measures appropriate to the risk, taking into account the state of the art. The requirements go far beyond those of the Telemedia Services Act, which since 2015 stipulates protective measures for all commercially used websites (Section 13 (7) TMG). The following aspects need to be considered:

1. **Security of systems and plants**
2. **Detection, analysis and management of security incidents**
3. **Business continuity management**
4. **Monitoring, audit and testing**
5. **Compliance with international standards**

The EU Commission has defined specific security elements for each of the five aspects by means of an implementing regulation.

Regular proof of the security measures taken toward the BSI is not required. The approach of "ex-post regulation" was deliberately chosen here, since effective risk and security management for a digital service is in the interest of the provider anyway. In justified cases, e.g. in the case of security incidents, however, the BSI can request appropriate documentation and insist on the removal of any security deficiencies.

REPORTING SECURITY INCIDENTS

If a digital service is affected by an IT malfunction or cyber-attack, it can have a significant impact on professional or private users of the service. Particularly in the case of cyber-attacks, it can often not be ruled out that even more providers could be the focus of the attackers.

As a result, digital service providers are required to promptly report security incidents with "significant impact" to the BSI. The corresponding criteria and thresholds for defining significant impacts were also set in advance by the EU Commission. They take into account both financial loss incurred by individual users as well as the total duration of defaults and the number of affected users in the event of data theft or sabotage.

ACTIVITIES OF THE BSI

The BSI has set up an information service for providers of digital services on its website. Questions about the regulation are also answered by the responsible office in the BSI (see infobox).

Companies should also be able to source the BSI's warning and information distributors in the future – in line with Critical Infrastructure Providers. Voluntary registration will be necessary for this. Furthermore, a working group is planned to promote exchange between the BSI and companies. ■

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

Office:
digitale.dienste@bsi.bund.de
0228 / 999582 6656

CYBER SECURITY

Getting Started – Made Easy

By Katrin Alberts and Holger Schildt, Section IT-Grundschutz

Basic Protection according to IT Grundschutz

The BSI's Basic Protection offers smaller businesses and public authorities along with self-employed people easy access into a security process according to IT-Grundschutz. Those responsible are able to use a guide to review and improve the status of information security in their institution in three steps.

Surveys such as the most recent cyber security survey conducted by the Alliance for Cyber Security (see page 22/23) show again and again that awareness of information security is commonly present despite a continuing lack of implemented measures to increase the level of security. Dialogue with small and medium-sized companies and self-employed people usually produces the same picture: there is often (still) a lack of trained personnel, necessary expertise and financial leeway to implement necessary measures in a sustainable and meaningful way. Secure data storage and Basic Protection of PCs, tablets and smartphones against unwanted external access are important to many people in management positions. However, the hurdle to clear, to actually deal with security aspects, is often still too high.

PRACTICAL SOLUTION FOR INSTITUTIONS OF ALL SIZES

This is exactly where Basic Protection comes in. As part of the IT-Grundschutz methodology, it is an entry point for all companies and authorities to secure their IT systems and information. It provides a compact and clear introduction to the development of an information security management system (ISMS) in an institution. This is a planned and organised approach to achieve and maintain an appropriate level of information security.

Basic Protection is based on the tried and tested BSI-Standard 200-2 (IT-Grundschutz Methodology) and explains elementary steps with which the level of information security in an institution can be checked and increased. It focuses on practical security requirements with the aim of keeping the entry hurdle to the security process as low as possible and avoiding all complex procedures. Besides technical aspects, infrastructural, organisational and personnel issues are also considered in the context of an integrated management system for information security. Basic Protection therefore enables a minimum of information security based on modernised IT-Grundschutz across all business processes and specialised procedures.

In smaller companies or public authorities, as well as for the self-employed, it is often a particular challenge to name a person responsible for information security issues. If the

THREE STEPS TO INFORMATION SECURITY

The process of increasing the level of information security is divided into three steps according to Basic Protection.

1 First of all, it is necessary to determine who will be responsible for the entire process. The first considerations also focus on restricting the scope of the ISMS. Which IT systems need to be checked? Which ones can be excluded, and why?

2 In the next step, security objectives must be specified and set down and a guideline must be drawn up. The management or management level should always be involved at an early stage. The organisation of the security process primarily involves designing and planning. For example, knowledge and security safeguards have to be integrated into existing processes and procedures. Applications that are "suddenly" secure but constantly crash are not very helpful.

3 The third step is to carry out the security process. The core task is to implement the previously defined security concept. Depending on the size of the institution modules on individual topics from the IT-Grundschutz compendium can be used for this purpose.

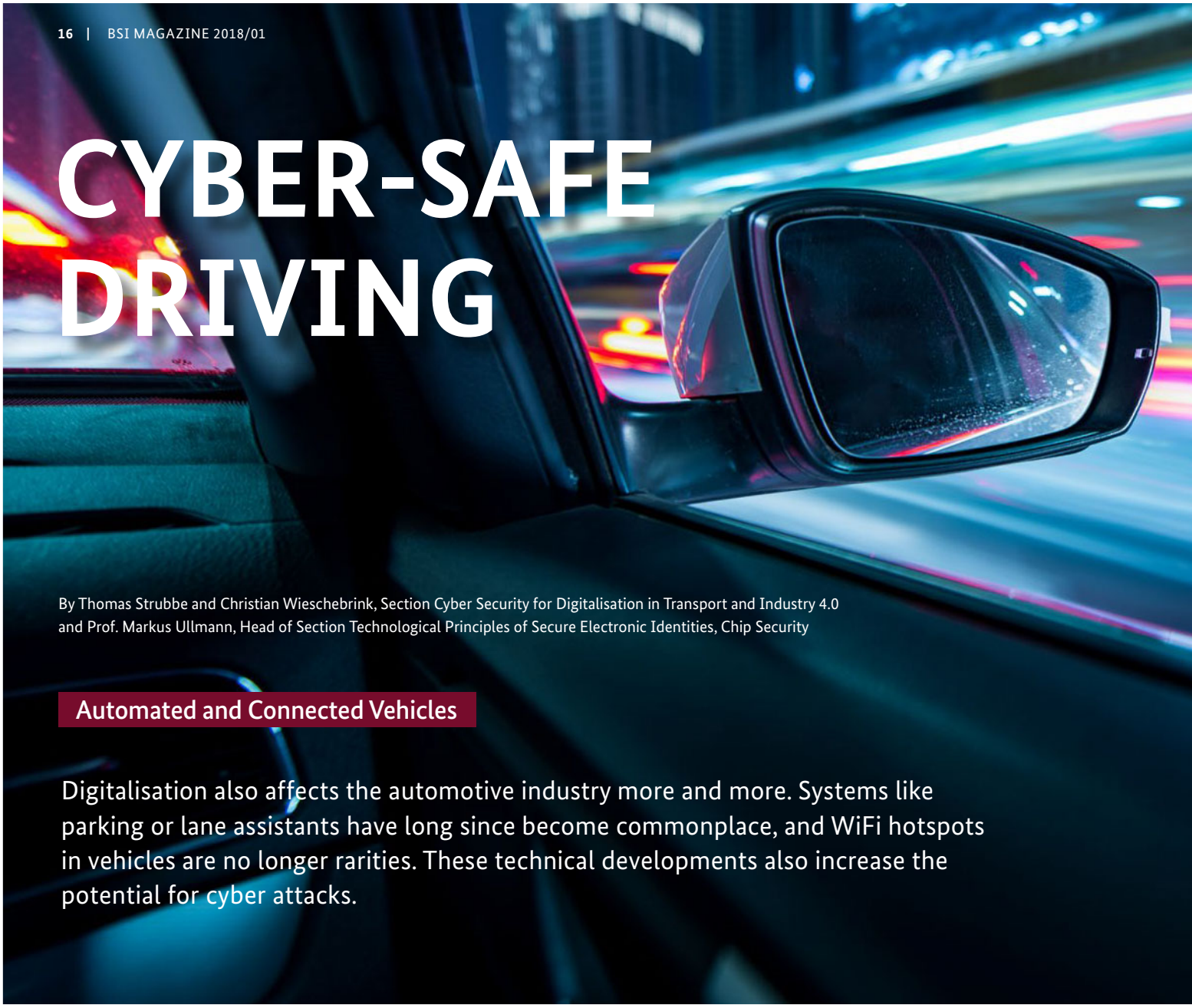
institution is somewhat larger, the task usually falls to a dedicated Information Security Officer (ISO). This role must also be established in smaller institutions. However, this is a task that an employee can take on in addition to other tasks. For example, employees from the areas of finance and controlling, IT operations or the company's data protection officer could take over these functions.

PRACTICAL RECOMMENDATIONS FOR ACTION TO READ UP ON

In a first step, the most important security requirements can be implemented quickly with Basic Protection. Your level of security can be further increased on top of this at a later date, for instance by protecting all areas with standard protection or critical business processes with core protection. ■

More information: basic coverage as a starting point for institutions of all sizes can also be found in a handy guide as a print brochure and online on the BSI website at https://www.bsi.bund.de/grundschutz

CYBER-SAFE DRIVING



By Thomas Strubbe and Christian Wieschebrink, Section Cyber Security for Digitalisation in Transport and Industry 4.0
and Prof. Markus Ullmann, Head of Section Technological Principles of Secure Electronic Identities, Chip Security

Automated and Connected Vehicles

Digitalisation also affects the automotive industry more and more. Systems like parking or lane assistants have long since become commonplace, and WiFi hotspots in vehicles are no longer rarities. These technical developments also increase the potential for cyber attacks.

In many vehicle models available on the market today, an internet connection via mobile radio is part of the standard equipment. New technologies such as vehicle-to-vehicle communication and eCall increase the degree of connectivity. Manufacturers are announcing that they intend to launch highly automated vehicles on the market in the foreseeable future.

Policy-makers see a great need for action when it comes to the Cyber Security of such highly connected vehicles. The Federal Government's "Strategy for Automated and Connected Driving" explicitly points out that accurate IT Security standards are needed, especially regarding vehicle approval. The BSI is actively participating with the Federal Ministry of Transport and Digital Infrastructure (BMVI) in the development of relevant criteria and the future orientation of Cyber Security in road traffic.

VEHICLE HACKS

While attacks on vehicle electronics in the past were primarily aimed at stealing the vehicle, developments in recent years have shown that the potential for attack has gone much further.

A number of further attacks on vehicle systems have been made public which show the dangers to which connected vehicles are exposed. For example, it was demonstrated that attackers could interfere with driving functionality over an internet connection via poorly secured infotainment modules in the vehicles. Certain smartphone apps that control vehicle functions such as opening doors or retrieving vehicle information also vulnerable to specific attacks.

In its own investigations, the BSI identified weaknesses affecting driver privacy. That includes the identification of

vehicles using Bluetooth signals as well as weaknesses in the pseudonymisation functions of future vehicle-to-vehicle communication.

ABSTRACT REFERENCE ARCHITECTURE

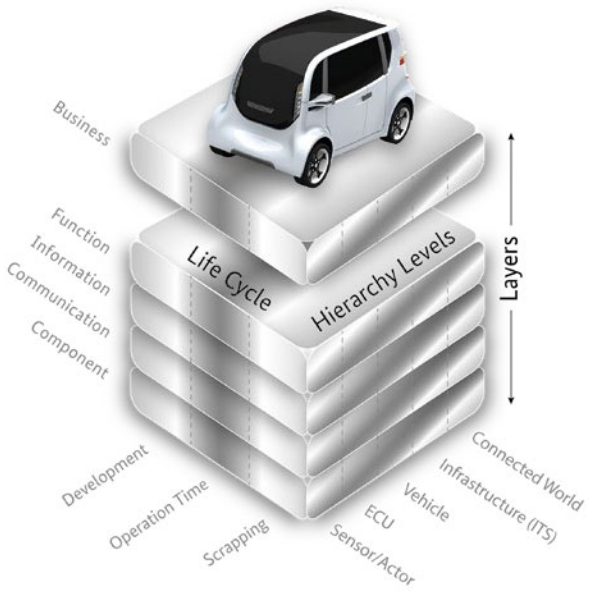
In order to investigate and discuss comprehensive questions on IT Security in vehicles, an architecture model is needed that is independent of models and manufacturers and does not assume a specific IT architecture in the vehicle. The "Reference Architecture Model Automotive" (RAMA) was developed with this aim in mind (based on RAMI 4.0, DIN SPEC 91345).

RAMA is a result of cooperation between industry, associations and authorities within the IT Security subgroup (UAG IT Security) of the BMVI and the BSI.

RAMA considers the vehicle in three dimensions:

- **Hierarchy levels:** these classify the vehicle from small units such as sensors and vehicle computers to the vehicle as a whole to the connected world.
- **Layers:** these describe components from the hardware level to application.
- **Lifecycle:** A distinction is made here between development, operation and ultimately scrapping.

The ability to break down RAMA into the required individual blocks makes it possible to model and examine manufacturer-independent IT functionalities at an abstract level.



Result of the cooperation between industry, associations and authorities: the architecture model RAMA

RAMA has been put forward as a proposal in the corresponding working groups of the United Nations Economic Commission for Europe (UNECE), in which requirements for the type approval of vehicles are defined that are currently valid in the 54 contracting states of the UNECE Convention.

OUTLOOK

The current developments in the automotive industry will entail new requirements for both automobile manufacturers and legislators. An attack on a fully automated vehicle would not only have consequences for its occupants, but could also endanger those in its environment. There must therefore be appropriate approval criteria for vehicles. This may include a suitable certification concept.

With the aim of international standardisation, the industry is currently developing a procedure model for cybersecurity engineering in vehicles (ISO/IEC WD 21434), which includes the development phase and security management in the field.

Another demand of the BSI is the protection of vehicles over their entire life cycle. For example, cryptoagility, or the migrability of cryptographic methods implemented in components, should be taken into account at an early stage of the development process. This also includes secure update mechanisms (e.g. for security patches) over a vehicle's lifetime. ■

More information:
Federal Government strategy for automated and connected driving
https://www.bmvi.de/SharedDocs/EN/publications/strategy-for-automated-and-connected-driving.html
https://www.bmvi.de/SharedDocs/DE/Artikel/LA/internationale-harmonisierung-der-technischen-vorschriften-fuer-kraftfahrzeuge.html

Security for Developers

By Dr. Peter Birkner and Dr. Aron Gohr, Section Evaluation of Cryptographic Mechanisms and Research Coordination

Technical Guideline for Cryptography

The BSI has been issuing guidelines with recommendations for the use of cryptographic primitives as part of TR-02102 since 2008. On the one hand, they contain general cryptographic recommendations covering the most important aspects of the development of cryptographic applications that are relevant to current practice. On the other, they provide concrete recommendations on how to use and configure certain cryptographic protocols. The following article describes the history of these Technical Guidelines (German: Technische Richtlinien, or TR for short) and highlights their current role in the context of other cryptographic standards and guidelines.

"The guideline facilitates the development or configuration of cryptographic systems."

The first version of the Technical Guideline TR-02102 from 2008 only gave general cryptographic recommendations on the choice of key lengths and cryptographic mechanisms. These recommendations – today's Part 1 of the TR – were primarily aimed at the developers of new cryptographic applications.

At the beginning of the current decade, it became clear that the TR no longer adequately reflected the changed framework conditions under which cryptographic techniques were used. On the one hand, this was countered by a fundamental revision of the TRs in 2012 and on the other by an extension of their content, leading to a division of the directive into initially two and now four parts.

While TR-02102-1 continues to provide basic recommendations on the choice of cryptographic procedures and key lengths, the other guidelines in the series provide practical guidance on how to configure cryptographic protocols, as may be of interest to system administrators for instance. Part 2 deals specifically with using TLS, Part 3 with IKE/IPsec and Part 4 with SSH.

All parts of this Technical Guideline have also been published in English since 2016, reaching an international audience of users and readers.

OBJECTIVES OF THE TECHNICAL GUIDELINE

Generally speaking, the four parts of TR-02102 can be considered a recommendation. They are intended to facilitate the development or configuration of cryptographic systems that correspond to the current state of the art. However, there is no institutionalised testing scheme that checks cryptographic systems against the TR. For example, within the scope of the BSI's approval procedures, deviations from TR recommendations are possible if they are necessary

and can be adequately justified with regard to the security properties achieved in the respective product.

Such deviations are not automatically detrimental to the security of an application; there are many cryptographic methods that are considered secure and relatively well studied but not recommended in TR-02102. The TR only deals with those mechanisms that are considered by the BSI to be particularly relevant. Figuratively speaking, the TR is more of a cryptographic kit with readymade parts that are known to be very strong than it is an encyclopaedia of everything currently considered secure.

"A security level of 100 bits is strived at – as of 2023 it will be 120 bits."

EFFECT OF THE TECHNICAL GUIDELINE

Although TR-02102 only contains recommendations, there are contexts in which these recommendations become binding. One example of this is the "BSI minimum standard for the use of the SSL/TLS protocol by federal authorities." This was first published in 2014 in accordance with Section 8 (1.1) BSIG and makes the currently valid version of TR-02102-2 for the use of TLS binding for federal authorities.

TR-02102 has a significant influence on approval and certification processes. As far as regards approvals, TR-02102 provides the manufacturer with a guideline, e.g. for the parameterisation of cryptographic mechanisms. However, this does not replace an overall assessment of the product by experts in the course of the approval process. For Common Criteria certifications in the German certification scheme, cryptographic algorithms and mechanisms are granted a security level of at least 100 bits (usually in the certification report) if they follow the recommendations of TR-02102.

An indirect effect also results from the fact that further Technical Guidelines from the BSI refer to TR-02102 and may be binding in their scope of application. This applies, for example, to TR-03116, which in four parts defines binding guidelines for the use of cryptographic mechanisms in federal government projects. For the evaluation of the security of cryptographic mechanisms, TR-03116 relies on TR-02102.

SECURITY OBJECTIVES AND CONTENTS OF THE TR

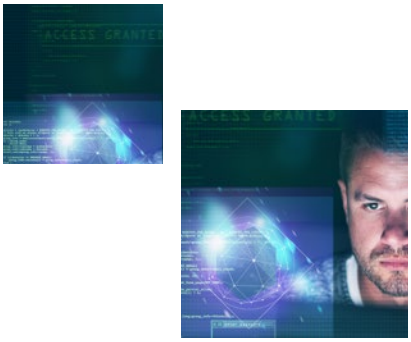
As a rule, TR-02102-1 strives for a security level of 100 bits. From 2023, this will become 120 bits. That means that there must not be a known attack on recommended methods the cost of which is less than the (classical) brute-force attack on an idealised block cipher with the corresponding key length. The recommended cryptographic methods and the choice of security parameters correspond to this goal.

Based on the recommendations given in TR-02102-1, the subsequent parts of TR-02102 derive guidelines for the secure use of specific cryptographic protocols. This pertains primarily to selecting the correct key lengths and other security parameters of the implemented protocols as well as secure cipher suites and to preventing specific attacks against the protocols. Fundamentally, isolated compromises of a system should also be prevented from causing a long-term loss of security of communications routed through the system. This is achieved by consistently recommending the use of cipher suites with Perfect Forward Secrecy, as long as there are no compelling reasons for using a configuration without this property.

POSSIBLE APPLICATIONS

The recommendations of TR-02102-1 are primarily intended as a resource for developers enabling them to select secure cryptographic methods. For example, if a software is to be provided with a function for creating electronic signatures, TR-02102-1 can provide an overview of the mechanisms currently considered to be secure. A concrete procedure and suitable security parameters, such as key lengths, can then be selected from these.

Parts 2 to 4, on the other hand, are intended for administrators who use cryptographic protocols and want to install, configure and operate software for this purpose. An example of such an application scenario is configuring a web server to use TLS. The administrator can make a variety of settings, some of which may influence the security of their web site and their users significantly. TR-02102-2 lists



specific cipher suites and key lengths, but also provides information on other security-related topics, such as selecting suitable random bit generators and certain attacks.

TR-02102 basically contains no statements on specific implementations. Nevertheless, the compatibility of implementations with TR-02102 can be checked. As part of a security analysis of the OpenSSL library commissioned by the BSI, various security aspects of OpenSSL were also examined from the perspective of TR conformity.

CONCLUSION

The BSI's cryptographic Technical Guidelines can provide the user with a basic orientation for selecting secure cryptographic mechanisms and configuring cryptographic solutions. Since their introduction, their focus has expanded from serving purely developers to the needs of administrators (application configuration).

However, adherence to the TR cannot replace the involvement of experts in the development or roll-out process of a cryptographic system. The security of a complete cryptographic system is influenced by many factors that cannot be reduced to the algorithms used. In addition, the security objectives and operating conditions of a particular system can lead to security vulnerabilities, for instance at the protocol level, even if cryptographically secure components are used.

Consistent consideration of TR-02102 by the developers or configurators of a cryptographic system can, however, make the task of an expert much easier, because at least the security of the basic building blocks and the basic security parameters used can then be easily assessed. ■

More information:

TR02102, Cryptographic Mechanisms: Recommendations and key lengths: https://www.bsi.bund.de/EN/TR

Study "OpenSSL library", Executive Summary https://www.bsi.bund.de/EN/OpenSSL_library

Contact Point and Exchange Platform

By Frauke Greven and Till Kleinert, Section Cyber Security for the Private Sector

Allianz für Cyber-Sicherheit

Alliance for Cyber Security is Increasingly Targeting Craft Enterprises

The Alliance for Cyber Security has provided large and small companies with extensive know-how and opportunities for dialogue on all questions and issues of IT Security in the digital age since 2012. In 2018, it will pay extra attention to the craft industry in Germany.

March 2012: The Industry Association for Information Technology, Telecommunications and New Media (Bitkom) and the Federal Office for Information Security (BSI) announced a joint press conference in the convention centre at CeBIT. The Alliance for Cyber Security was born. Under the auspices of the BSI, a range of information was created, aimed in particular at small and medium-sized enterprises, offering practical help in protecting against and responding to cyber attacks. Its content comes not only from the BSI itself – experts from the business world are also cordially invited to get involved as partners of the Alliance for Cyber Security and to provide

their own content. Participants of the initiative can thus increase their own security level with the help of proposed measures. In return, they provide empirical values from operational practice as well as reports of actually observed incidents. The result is a collaboration in the form of a public-private partnership that benefits everyone involved.

MORE THAN 2,600 MEMBERS TODAY

Today, more than 2,600 companies and institutions belong to the Alliance for Cyber Security. New applications every day show that the idea of a cyber security contact point is in line with the times. Besides information on the platform www.allianz-fuer-cybersicherheit.de, the alliance partners offer seminars and workshops on various topics in numerous locations. The Cyber Security Days of the Alliance for Cyber Security are organized quarterly, now at intervals of two months throughout Germany. Each event has a relevant guiding theme in IT Security.

THE FUTURE IS LOOKING TOWARDS CRAFTSMANSHIP

Digitalisation has progressed since the creation of the Alliance for Cyber Security. Sites, processes and machines are connected with each other, not only in global corporations, but computers and programmable control components have also long since entered centuries-old, originally entirely analogue productions and processes.

For this reason, the Alliance for Cyber Security is addressing the many craft enterprises in Germany in 2018. They not only face the challenges now almost normal for today's working world such as going to the cloud or dealing with mobile devices, but also have to deal with protective measures for computer-aided special machines in areas such as production and construction. Experiences from diverse projects, construction plans and customers and supplier data make craft enterprises attractive targets for cyber attacks.

The German Confederation of Skilled Crafts (ZDH) and the BSI agreed on increased cooperation in late 2017. The 20th Cyber Security Day on 25 January 2018 was the first event specifically aimed at craft enterprises. Through various presentations, participants were able to find out about the latest cyber threats and protective measures.

Key elements in the fight against cyber attacks include modernised IT-Grundschutz from BSI. In the coming months, IT-Grundschutz profiles will be developed that can be used by individual companies as a blueprint for implementing security measures. More offers are planned throughout the year. These include information campaigns, industry-specific events and multiplier training. The aim is to strengthen expertise in IT and data security in the companies and provide valuable practical information on the prevention and defence against cyber attacks. ■

"More than one million craft enterprises are a significant factor for Germany as a business location. Digitalisation is also on the rise in craftsmanship, for instance in project planning, in the control of previously manually operated tools and in administrative procedures. As connectivity advances, craft enterprises are also facing hacker attacks, malware, phishing and other cyber risks that can lead to data loss, production losses and financial damages. As a National Cyber Security Authority, the BSI works hand in hand with the ZDH and supports craft business in overcoming the challenges of digitalisation."

Arne Schönbohm, President of the BSI

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

SPECIAL FEATURE

Industry 4.0 – Security by Design

By Arne Schönbohm, President of the BSI

The global economy continues to interconnect. The globalisation process of the markets is primarily driven by new technologies in the areas of communication, information and transport. Global data networks, satellite communications, computer-aided logistics and the most advanced means of transport enable companies to select the most favourable production and delivery locations. The greatest market potential, however, does not lie in the choice of location, but in increasing the efficiency of production processes through the use of intelligently connected systems.

Industrial control systems are already in use today in automated control, regulation and measurement. Users range from the manufacturing industry to the chemical industry and Critical Infrastructures; they include small and medium-sized firms as well as large companies and international corporations.

For many of these companies, it is becoming increasingly important to exchange information as quickly and directly as possible within the company, with other branches or subsidiaries abroad, with suppliers or customers. To achieve this, areas that were previously physically separated from each other are connected over the Internet – and can therefore be attacked. Data flows are the capital flows of digitalised business. If they are disturbed, everything comes to a halt.

This makes it all the more important to create sustainable security awareness in business culture to lay a solid foundation for digitalisation. Only if Cyber Security is taken into account by design can companies successfully participate in digitalisation and avert damage right from the start.

Recent years have shown more than once how particularly worthy of protection industrial control systems are and what consequences attacks on these structures can have. In December 2015, for instance, at least 225,000 people in the Ukraine were affected by a power outage lasting several hours caused by a targeted cybe rattack. In December 2016, there was another power failure in Kiev, the Ukraine's capital. According to the managing director of the state energy provider, this also was caused by a targeted cyberattack. Between 100,000 and 200,000 inhabitants went without electricity supply for over an hour. Another example is the massive adverse effects of the ransomware "WannaCry" on the Danish logistics company Maersk as well as various other production companies. At Maersk alone, the damage is estimated at around 300 million dollars.

A digitalised society can only function sustainably with information and Cyber Security that is consistently proportional to the risks. This security can come in part from the close and trusting cooperation of all involved parties, and in part from the correct interaction of technical and organisational measures that complement each other

"Only if Cyber Security is taken into account by design can companies successfully participate in digitalisation and avert damage right from the start."

Arne Schönbohm, President of the BSI

from the very beginning. As the National Cyber Security Authority, the BSI has therefore set itself the goal of strengthening and maintaining proven German and European IT and security standards. BSI IT Grundschutz, a nationally and internationally recognised information management system, along with its compendium offer a comprehensive tool and reference for information security. It also specifies the requirements for safeguarding industrial control systems. On the other hand, the BSI is pushing for the principles of "Security by Design" to be consistently applied. They lay the foundation for safe products and technology and create a uniform, transparent level of security. Their implementation, however, must be verifiable and traceable, by receiving certification, for instance.

The BSI also participates in national and international initiatives such as Platform Industry 4.0 in support of secure concepts from their outset. Its membership in the Alliance for Cyber Security and its extensive information and awareness-raising events such as expert circles and Cyber Security Days make a significant contribution to overcoming the challenges of digitalisation and securing the success of Germany as a place of business. ■

Joint Responsibility

By Jens Mehrfeld, Section Cyber Security in Industrial Control Systems

Clear Communication of Security Requirements

In the age of Industry 4.0, Cyber Security is essential for plant and machine availability. The rising number of cyber attacks on production facilities highlights the need to act, but it is often difficult to know where responsibility lies. Personal responsibility and clear communication of requirements and application specifications are necessary to avoid this dilemma.

Many different companies get involved along the way from the conception to the operation of industrial plants and machines. It begins with the manufacturers of individual components such as programmable logic controllers and sensors. Mechanical engineers and integrators assemble these into machines and production systems. These are provided by an operator who uses and supports them. In the age of Industry 4.0, other players such as predictive maintenance or cloud services will be added. And each of these parties has their own specific interests:

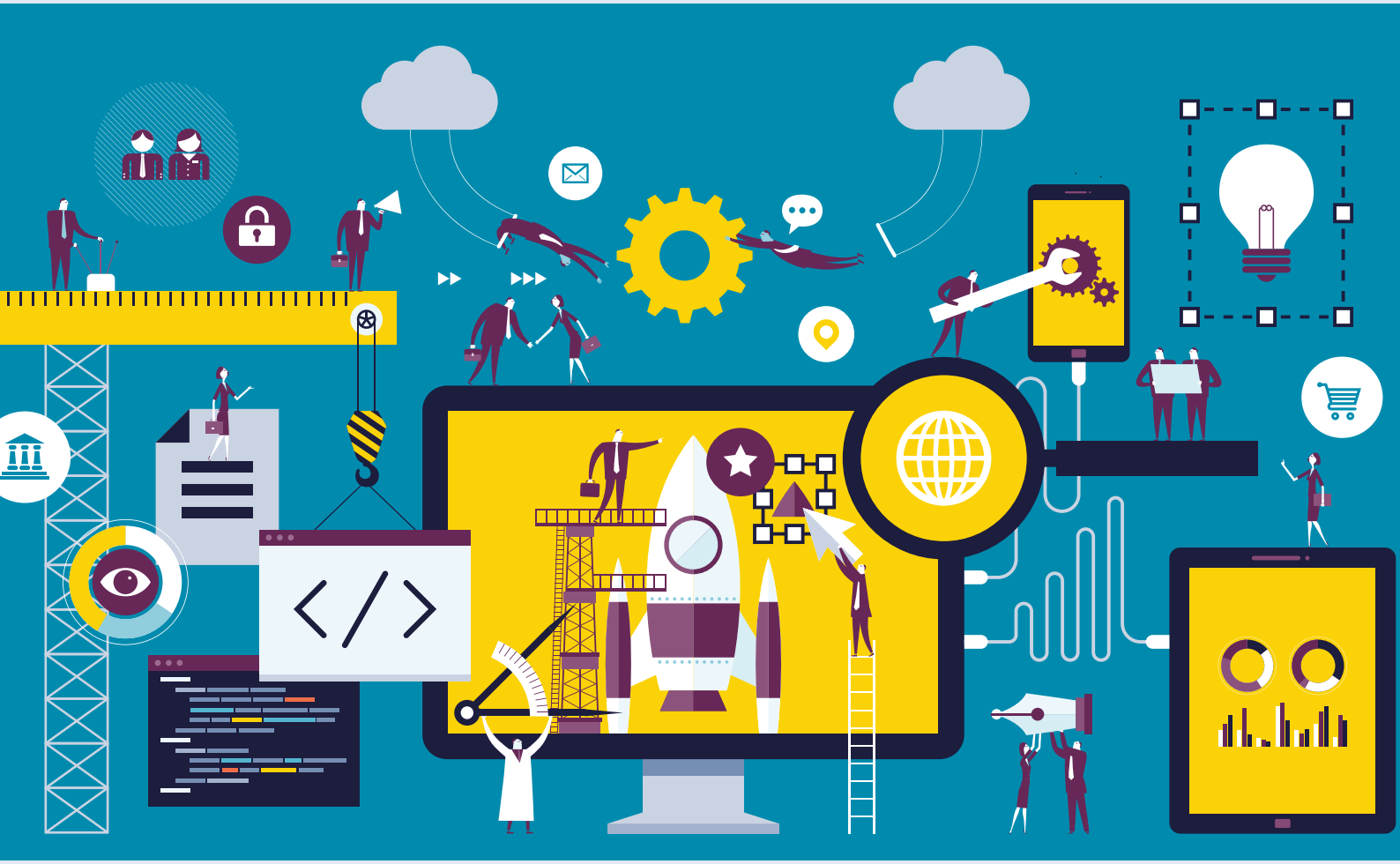
- Operators want to buy a cost-effective, flexible system with a long service life, low downtimes and that takes as little effort to operate as possible.
- Integrators want to plan, programme, commission and maintain systems quickly and with little effort. They take only the requirements of operators into account.
- Manufacturers offer components with many functions to enable a wide range of applications.

What everyone involved has in common is that they want to achieve the best possible result with as little time and money as possible. They focus on the actual functionality of the component or system.

THE DILEMMA OF CYBER SECURITY

Cyber Security is often regarded as an annoying or unnecessary additional effort and neglected as a result. Manufacturers are little concerned with vulnerabilities in their components, integrators do not use security functions and operators are not worried about security measures. This lays the groundwork for attacks on plant security.

Cyber Security is more than just protecting the confidentiality and integrity of information. It is also about the availability and integrity of systems and components and thus the availability of plants and machines. This can have dramatic consequences. Manipulation or malfunction of a component has a negative effect on production. This contradicts the interests of the operator. If he is dissatisfied with the system, he will likely look for another integrator for the job. The same applies to selecting components. Here, too, he will look for other possibilities that run counter to the



manufacturer's interests. This is why everyone involved should develop and cultivate one more common interest: Cyber Security.

COMMON TASK

Awareness of responsibility is on the rise – especially in the area of Critical Infrastructures. The IT Security Act lies behind this, with its obligations to establish an information security management system and to report incidents. Its tasks include risk management and the targeted implementation of protective measures. Manufacturers and integrators also need to implement an ISMS to protect their infrastructure along with their development and customer data. Manufacturers and integrators would also do well to attach significance to Cyber Security during development. This applies to both programming and design. When programming software, errors should be avoided and detected as early as possible. That can be achieved through guidelines for developers and accompanying tests. This initially incurs costs or slows down development to a certain extent, but it pays off in the long term. Possible errors are detected much earlier and can be corrected more cost-effectively. If a developer finds a bug before release, it can be fixed faster than if found afterwards. A new version would have to go through the complete release and quality assurance process again. This illustrates how Cyber Security measures reduce costs in the long term.

OPEN COMMUNICATION

The same applies to the open communication of requirements and application specifications. Operators make demands on integrators and integrators on manufacturers. Besides technical requirements, these demands should regard Cyber Security requirements as well. Protective measures already taken in the plant should be described. Requirements should be determined within the ISMS. Application specifications can also be made to integrators from operators or vice versa. These should contain instructions on the conditions under which safe operation is guaranteed. These instructions must be taken into account by the operator in the ISMS. Higher investment in the procurement of a system can quickly pay off in increased Cyber Security, since less effort is required during operation and system availability is not reduced by attacks. ■

Cyber Threats for Industrial Plants

By Andreas Erdrich and Jens Kluge, Section Cyber Security in Industrial Control Systems

Security by Design Allows Higher Resilience against Attacks

Cyber attacks on industrial control systems (ICS) are often similar to common attacks on IT systems, but can have physical effects. In the worst case, production of essential goods is lost, people and the environment are threatened and critical infrastructures are impaired. Potentially affected systems therefore need special protection. In an increasingly connected environment, “Security by Design” offers basic immunity from cyber attacks.

IT AS AN ATTACK TARGET – WITH EFFECTS ON MACHINES AND SYSTEMS

In the field of Operational Technology (OT), Microsoft Windows is used as an operating system in many systems such as industrial PCs and Human Machine Interfaces (HMI) as well as on development and project planning computers. There is a large number of malware for this operating system because of its widespread use. And in contrast to IT in office environments, patches and security updates on these systems are often not applied at all or only with great delay due to high availability requirements. The Conficker, WannaCry, NotPetya and Copperfield malware shown in the figure above are all examples of the major long-term threat potential posed to these systems and equipment.

These malware variants do not target ICS directly; therefore, failures are considered collateral damage. Effects on industrial processes, however, can be serious if components such as HMIs fail (loss of view) or important process data can no longer be accessed (loss of control). WannaCry and NotPetya, for example, have caused and continue to cause companies and plant operators operational disruptions and breakdowns lasting several weeks, which has led to image damage and sales losses in the millions for those affected.

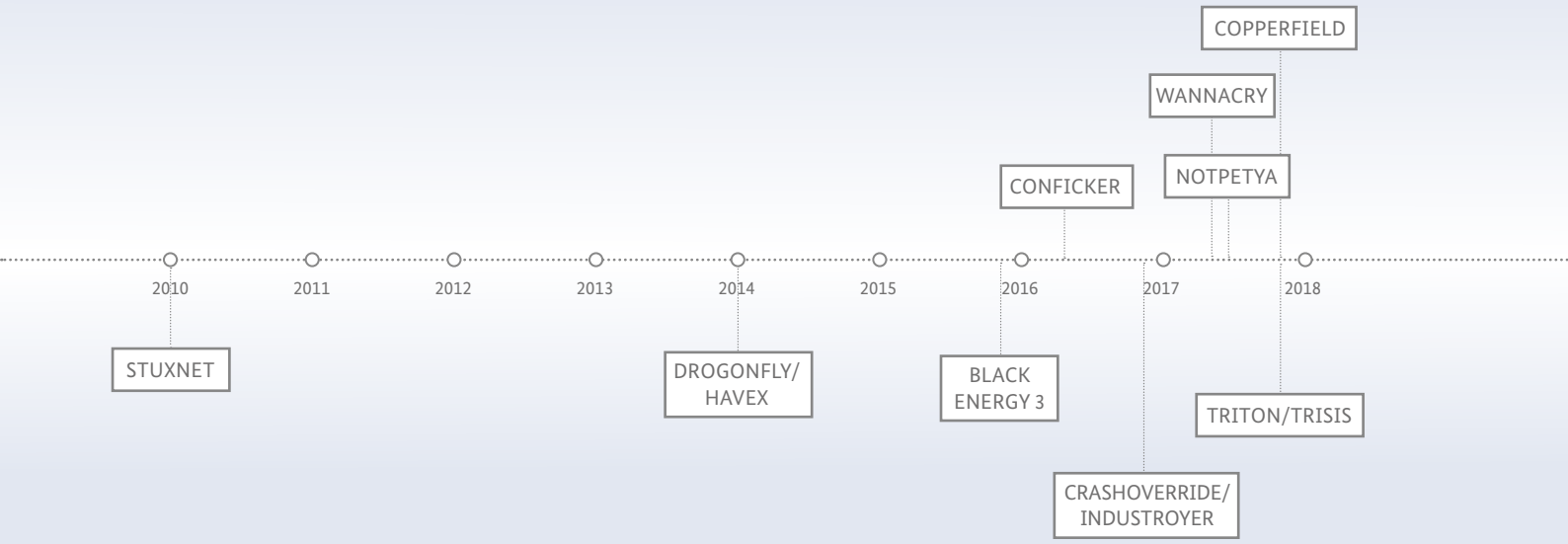
THE TIP OF THE ICEBERG – TARGETED ATTACKS AGAINST ICS

There have also been a number of known incidents in recent years of malware targeted against industrial processes. These often required in-depth knowledge of plant configuration and considerable resources for preparation and implementation. This suggests that criminal or state-oriented organisations lie behind the attacks.

- Stuxnet aimed to sabotage the process of uranium enrichment in a plant in Iran by mechanically damaging gas ultracentrifuges by specifically changing the speed and process pressures. Process visualisation was changed during the attack to such an extent that a previously recorded period of several days was installed. What was remarkable about Stuxnet was that the malware had to find a special plant configuration in order to become active. As a consequence, manipulation only took place in the Iranian plant despite the worldwide spread of the malicious code. The use of several zero-day exploits suggests a high financial expenditure on the part of the attackers.

- The Dragonfly campaign was designed to collect and exfiltrate confidential data from ICS. The malware

TIMELINE OF TARGETED (TOP) AND NON-TARGETED (BOTTOM) ATTACKS ON ICS



Havex it used was a remote access Trojan distributed in three different ways: spear phishing mails that contained the malware, watering hole attacks that redirected visitors to websites with exploit kits, and the infection of legitimate software from three different ICS component vendors. More than 50 variants of the Havex Trojan were found and at least 2,500 people affected. The malware scanned networks on ports of ICS-specific protocols and searched for OPC servers, among other actions. It also exfiltrated VPN configuration files, browser passwords, address books and user/system information.

- Black Energy 3 was an attack on the power supply in the Ukraine, putting up to 700,000 people without electricity for several hours. Three energy companies were affected, where the control systems for the substations and switchgear were sabotaged in a coordinated manner every 30 minutes. This eventually led to the blackout. Remarkably, the malware had remained undetected for almost eight months before the attack, giving the attackers plenty of time to explore the facilities and further develop the attack.

- A year later, Industroyer/Crashoverride is said to be the cause behind another brief blackout in the Ukraine, this time in the Kiev region. The power supply was able to be restored by manual intervention in the switching stations after almost an hour. Later analyses using samples of the malware revealed a modular structure and a targeted alignment of the malware code to the telecontrol protocols commonly used in power distribution with the aim of triggering the switches for network separation in medium and high-voltage systems using the respective controls.

WHAT SHOULD WE EXPECT TO FACE NEXT?

Despite their sophistication, these targeted incidents represent only a fraction of the industrial damage caused by malware. The greater part still comes from non-targeted attacks. The targeted attacks mentioned here are merely the tip of the iceberg.

Attackers benefit from the fact that many of the systems and communication protocols used in plants have been in use for decades. Once attackers have gained access to the OT system, it has hardly any protection against the attack. The progressive networking of the plant components along with increasing functionality offer access to additional attack vectors. The effects can be even more serious if not only the actual process but also the functional safety of the plant is impaired by an attack. That places people and the environment at risk, as described in more detail in the following article. ■

Security for Safety

By Erwin Kruschitz, anapur AG and Veselina Hensel, Section Cyber Security in Industrial Control Systems

No Hype, but Necessity

14 December 2017 promised to be a normal day until reports of the IT Security service providers FireEye and Dragos were published about a new malware. In a digitalised world, such reports are commonplace, but not when industrial control systems are involved. The extraordinary thing about this malware was that, for the first time, a Safety Instrumented System (SIS) was specifically manipulated, a system designed to avert threat from people, the environment and technical facilities.

Unknown perpetrators had managed to penetrate a company's network and gain control of one or more engineering work stations. At least one of them contained special software used for programming and parameterisation of the SIS in use. By loading malicious code onto this computer, the perpetrators were able to search the net for an SIS from a specific manufacturer, establish a connection to it and import malicious code built to manipulate the program logic of the SIS. Analysis of the attack and malware is still in progress. It has since become known that some of the perpetrators successfully made changes in ongoing operations. One of the systems reacted as intended, putting the system in a secure state and preventing more serious effects.

SAFETY VS. SECURITY

Discussions between IT Security experts and automation engineers often suffer from different ways of understanding how risk is defined in their respective contexts.

In connection with safety, risks arising from machinery and industrial processes and posing a danger to people and the environment must be reduced to a tolerable level. With IT Security, however, the focus is also on intent and targeted action.

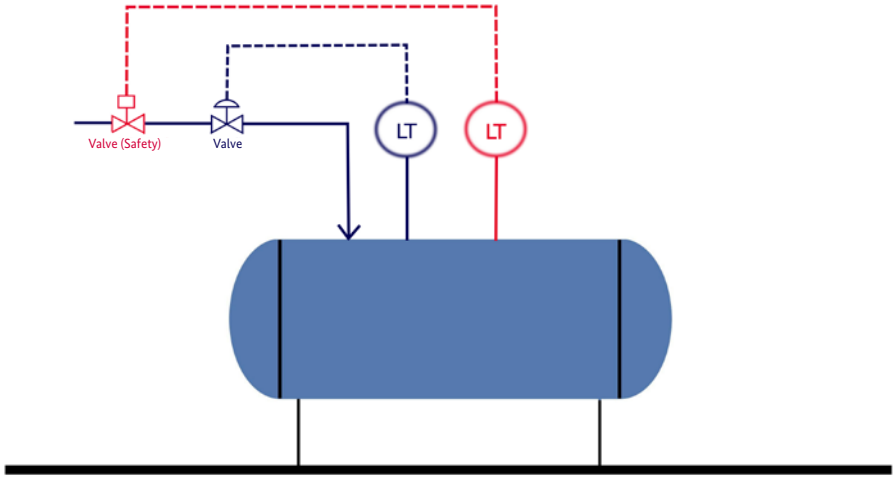
CONSIDERED ACTION NECESSARY

Since Stuxnet malware was discovered in 2010, Triton/Trisis/HatMan is now the fifth currently known malware specifically targeted to industrial control systems. This number may seem small, but it is no reason to sit back and relax. On the one hand, industrial plants are generally unique; on the other, security engineering is a discipline that requires highly specialised knowledge, so that highly developed, targeted attacks are complex and time-consuming. But they are possible. Not to be forgotten, untargeted attacks such as ransomware can also have high potential for damage.

SIS AND ITS TASKS

Safety systems form a subgroup of industrial control systems and are used to avert dangers to people, the environment and technical installations. A significant difference to conventional automation systems is increased demands on reliability.

SISs (shown in red) are used both in machines and in process engineering plants. They operate independently of control systems (shown in blue) that control a physical process or machine. The diagram shows how the risk of overfilling the container is countered by the Safety Instrumented Function (SIF) implemented in SIS: as long as the operation functions smoothly, the SIS takes on a purely observational function. However, if faults or deviations from predefined criteria arise, SIS intervenes in the process and puts the machine or system in a controlled and secure state. In this example, the valve is closed when the level sensor (LT) signals overfilling.



Action must be taken. Safety, after all, is useless without IT Security. Standards like IEC 61511 have been established based on this insight. The BSI has also been working on the topic for several years, for instance by actively participating in the creation of the Namur NA 163 worksheet. There is also a module within the scope of the IT-Grundschutz of the BSI that supports operators in the analysis, selection and implementation of measures for securing SISs.

The challenges for manufacturers and operators are great, since classic safety concepts and recommendations cannot simply be transferred. Safety components undergo special validation and certification processes so that plant modifications or product innovations are correspondingly rare. The long service life of machines and systems is another reason why manufacturers must actively take the risk associated with connectivity into account and allow it to flow into the entire life cycle.

Despite the risks, protecting people, the environment and the plant must be reliably guaranteed. Only then can digitalisation be successful. ■

More information, a simplified risk analysis and recommendations and steps to safeguarding SIS for operators:

NA 163 “IT risk assessments for PLT Safety Instrumented Systems” and the corresponding checklist: http://www.namur.net/de/publikationen/news-archiv/detail/article/na-163-ist-neu-erschienen.html

IT-Grundschutz Compendium of the BSI, module “Safety Instrumented Systems”: https://www.bsi.bund.de/IT-Grundschutz-Drafts

"Secure Identities: Necessary Starting Point for Business Processes"

Interview with Michael Jochem, Head of the "Security of Connected Systems" Working Group

How does Germany as a production location intend to further increase its competitiveness with Industry 4.0? What role does Germany play in setting standards? How can Industry 4.0 redesign the work world for the benefit of people? Platform Industry 4.0 deals with these questions, and a working group has taken up the topic of the IT Security of Industry 4.0. BSI Magazine spoke with Michael Jochem, Robert Bosch GmbH, Head of the "Security of Connected Systems" working group.

Mr. Jochem, what are the objectives of Platform Industry 4.0?

Companies, associations, politicians, scientists and trade unions work together to develop concepts and recommendations for action, provide orientation aids for small and medium-sized enterprises and shape international exchange – everything for a successful transition into Industry 4.0. We want to help ensure that Germany remains a leader in factory equipment in the future and further increases its competitiveness. Relevant trends and developments in the manufacturing industry are identified and brought together in the sense of a uniform overall understanding of Industry 4.0. IT Security plays a central role in that.

Why?

Data is the oil of the 21st century. Its storage and processing create added value. But unlike oil, data is very volatile. Stored and transmitted data has to be ensured as correct and complete. To this end, IT Security provides catalogues of measures, for example, to protect against unauthorised access, changes or unauthorised copying.

Organisation and processes play a decisive role here. Unlike in the analogue age, Industry 4.0 requires a holistic approach that includes office IT, product development and production IT. An information security management system (ISMS) supports management with implementation and serves to minimise company risk and meet regulatory requirements. IT Security therefore makes a significant contribution to business success.

Can you explain "secure identities" in more detail?

Of course. If business processes are to be made more flexible, secure identities are – for legal reasons – the necessary starting point for almost all business processes. Without secure identities, flexibilisation in Industry 4.0 would become impossible by default. Only those who trust each other (people and machines) should communicate with each other.

What does trust mean in this context?

It means how well you can rely on your business partner or a product. Does the business partner or the product do what he or she is supposed to do? Trustworthiness in the product context means that there are no hidden functions and that adequate protection against malfunctions and attacks is guaranteed. We do not yet have criteria or evaluation scales to assess this or to determine it automatically for a product. Increasingly automated processes with ad-hoc connectivity among each other require methods with which the trustworthiness of the participants can be determined and evaluated.

So secure identities are gaining central significance for the overall process?

Right. A popular example is any type of remote access. It may be necessary for condition monitoring of a machine or for

"Unlike in the analogue age, Industry 4.0 requires a holistic approach that includes office IT, product development and production IT."

Profile in brief:

Michael Jochem is currently responsible for IT Security governance and services as Director, Project Business Chief Digital Officer. He brings more than 30 years of automation technology experience from various functions (development, product management, sales) at Bosch Rexroth AG and Robert Bosch GmbH to the working group in Platform Industry 4.0.

maintenance and service. In any case, it must be ensured that only the authorised service technician or the monitoring systems have access. Secure identities can also help protect against counterfeit products by allowing the origin and authenticity of a component to be validated. So there is a wide range of applications. The publication "Secure Identities" from Platform Industry 4.0 shows the importance of secure identities, compiles the essential elements for the trustful establishment of value creation networks and derives recommendations for action. Managing organisational tasks such as identities or implementing information security management is a challenge for many companies.

Have you already considered this as well?

Yes, the guideline "IT Security in Industry 4.0 – Fields of Action for Operators" describes not only technical protection measures but also the organisational framework conditions for digitalised production. Known risks can be reduced by implementing the steps described and using the practical information, for instance on possible requirements when purchasing machines and systems. This lays the groundwork for being a trustworthy partner in value creation networks.

Processes and measures are implemented by people. How do you ensure that your employees have the necessary know-how?

That is indeed a critical point. For that reason, we have identified necessary IT Security competencies in training and continuing education in the working group and presented them in a publication. It describes competencies across all value-added partners and hierarchy levels and identifies the requirement profile of an Industrial Security Officer as the central contact for IT Security in production.

The findings of the publication have recently been incorporated into training occupations in the electrical industry, supported by ZVEI. They are to be implemented by August 2018. The basics will therefore already be taught during training.

How are you already addressing IT Security in Industry 4.0 at your company Bosch?

IT Security must be considered right from the start. The Bosch Security Engineering Process (SEP), which guides our product development, describes the necessary activities in the context of IT Security and data protection and thus ensures "Security by Design." An established network ensures the exchange of data in production and with other organisational units. And in the future, a standardised remote maintenance solution for more than 100,000 connected machines and systems will help to securely connect service technicians both internally and externally and reduce the target area.

We see appropriate IT Security and a high level of data protection as part of the Bosch quality promise. ■

THE BSI

Advantage Diversity

The BSI Promotes Women in MINT Professions

Public and private employers are equally committed to attracting qualified junior staff, especially if they have been trained in the so-called MINT professions. Math, information/computer science, natural science and technology (MINT) are still in the eyes of many a "man's business." The BSI has joined the "National Pact for Women in MINT Professions" to make sure that does not remain the case.

Just below 15 percent: according to the Federal Statistical Office, the share of female employees in the IT and ICT sector in Germany was this low in 2016. A number that no one is pleased about – neither politics nor business, nor the BSI as an employer.

There are many reasons for this, yet one always stands out: stereotypes. Computer science, for instance, is often referred to as a "typical male domain." The figures seem to confirm it, too, and yet there are always female role models (see the interviews opposite) to show that women belong in information technology and security.

The BSI wants to encourage female students and working adults to freely pursue this exciting field. No matter whether math, physics, electrical engineering, computer science, political science or economics, many disciplines at the BSI are contributing to the secure design of digitalisation. A big task for dedicated professionals – of whichever sex – to show their digital perspective.

WOMEN AT THE BSI

Across all of the BSI, the female employment rate is currently around 27 percent. In contrast, 35 percent of new employees hired in 2017 were women. The share of women as recent unit heads was 50 percent last year. A positive trend is clearly recognisable, as the share of female employees at the BSI significantly mirrors the industry average – but no one at the BSI wants merely average.

komm mach MINT
NATIONALER PAKT FÜR FRAUEN IN MINT-BERUFEN

In order to systematically target women for BSI positions, the national cyber security authority joined the "National Pact for Women in MINT Professions" in 2016, an initiative of the Federal Ministry for Education and Research with the slogan "Go MINT". In the medium term, membership should increase the share of female employees and executives at the BSI, partly through steps such as gender-sensitive personnel marketing and cooperation with local universities to promote the share of women in technical courses. ■

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


Yona Raekow


Ayse Yenigün

FOUR QUESTIONS FOR: YONA RAEKOW

What led you to join the BSI?
The BSI first came onto my radar in 2012. I applied and then worked on "Cryptography in applications" as well as "Evaluation of secure mobile solutions." I went through the in-house management trainee program and recently successfully applied for the position of Unit Head for IT Security Services Certification.

Women are still often considered "exotic" in the IT world. What inspired you to take this path nonetheless?
When it came time to choose my course of study, a bioinformatics program was being offered. I thought to myself, "I can do bio," and, "Computer science is exciting and completely new territory." I wasn't so exotic since some other women felt drawn to bioinformatics, too. It turned out that computer science was much easier for me than biology, and I ended up earning a master of computer science and engineering degree in the US.

You are married, have two children and now work in certification management. How do you pull it all off?
My husband also works at the BSI, which is a big help for coordinating family and work. The flexible working hours and part-time opportunities are especially helpful in making it possible to reconcile our professional and private lives. In my experience, I've also found that co-workers and supervisors are very understanding when there are challenges at home.

What would you like to impart on students and newcomers interested in information technology?
That they are interested in an exciting and diverse career area and should try out as much within it as possible. And I'd like to offer something to those who are not (yet) interested: just give it a chance, it's really fun and it's not rocket science.

FOUR QUESTIONS FOR: AYSE YENIGÜN

How did you find your way to the BSI?
In a roundabout way. I first trained as a medical assistant and then decided to study computer science. I then found my way into the BSI through my master's thesis and applied after graduation. I've now worked in the National IT Situation Centre since 2016.

From the doctor's office to the National IT Situation Centre – how did that happen?
A dream of mine was to be part of something on a big scale and to do something for the greater good. These and other reasons led me to initially decide to train as a medical assistant. Computers were my constant companions. Through the constant use of information technology, I realized that what was originally just interest in the underlying science had turned into curiosity. I studied computer science, which brought me closer to my goal of being able to let my knowledge make a difference. Now for the "happy ending," I'm part of a big team where I can use my skills for National Cyber Security. I also have the opportunity to expand my knowledge every day at an exciting job and in a great environment.

Computer science students have a lot of open doors after graduation right now – what inspired you to join the BSI?
IT Security was the most interesting issue for me. It's also important for me to work somewhere exciting and diverse. I also don't want to feel competitive where I work, but to have a team spirit where everyone sticks together and works for the same goal. I'm personally developing along with IT Security, so where could I be better off than at the BSI?

Studying computer science is very demanding – what tip can you give freshmen and high schoolers for handling it successfully?
Learning by doing. Try everything theoretical and don't just hope for quantum leaps. Computer science works best by applying it and learning it step by step. This is motivating because it leads to very many feelings of success along the way, and what you learn sticks with you for life.

Expanding the Cooperation with Federal States

By Stefanie Euler, Section IT Security Consulting for Public Authorities and Fabienne Middeke, Head of Section National Liaison Office

Create a Uniform Level of IT Security

Through its IT Security consulting and national liaison office, the BSI is continuously expanding its cooperation with the federal states. Its underlying goal is to create a uniform level of IT Security. This is even more important with regard to the progressive digitalisation of administration and the increasing connectivity of IT structures between the federal and state governments. First declarations of intent were signed last year with Rhineland-Palatinate and Hesse, and this year with North Rhine-Westphalia.

As the National Cyber Security Authority, the BSI designs Information Security in digitalisation through prevention, detection and reaction for government, business and society. In order to comprehensively pursue this nationwide approach, the Cyber Security Strategy for Germany 2016 set out to strengthen cooperation between the federal government and the states. Section 3 of the BSIG (Act on the Federal Office for Information Security) lays out the legal basis for this. The BSI advises and warns states on Information Security issues and assists them in securing their information technology and averts threats at their request.

Besides the mandate from the Cyber Security Strategy, a decision by the federal and state interior ministers and senators in 2017 is also of major/crucial/high importance for the BSI's cooperation with the states. Therein, it is emphasised that improved institutionalised cooperation between the federal government and the states was necessary for IT Security. The BSI "with its recognised competence and available resources" was given particular importance in this process.

STRUCTURES OF COOPERATION

Within BSI, structures at advisory, strategic and operational level exist in order to shape cooperation between the federal government and the federal states in the area of IT Security:

Cooperation between the federal states and the BSI is also strengthened by the Act Implementing the EU Directive on Network and Information Security (NIS Directive). According to Section 3 (1.2.13a) BSIG (Act to Strengthen the Security of Federal Information Technology), the BSI may now support relevant state authorities at their request in averting threats to the security of information technology and may provide technical expertise. The BSI is therefore the federal authority that supports the federal states in emergency response in the area of Cyber Security.

States may also cooperate with the BSI to develop regional concepts for business protection.

Since September 2017, President of the BSI Arne Schönbohm has signed declarations of intent with Rhineland-Palatinate (State Secretary Randolf Stich, top left), Hesse (State Minister Peter Beuth, bottom left) and North Rhine-Westphalia (Economics and Digital Minister Prof. Dr. Andreas Pinkwart, top right)

The BSI's security consulting is its central contact point for consulting inquiries from federal and state government in the context of information security management (ISMS). It is the central point of contact for information security officers from the respective authorities and receives proper insight into the information security situation "on site" through committee work, close contacts with authorities and an efficient exchange of information on IT Security. Security consulting supports the information security officers of authorities in the process of introducing an ISMS or finding balanced approaches to solving information security matters.

The BSI's National Liaison Office shapes the BSI's relations with national partners in the fields of government, business and society. Its special feature is its regular presence in selected regions of Germany. This facilitates direct exchange and creates concrete accessibility to the BSI on site. The expansion of cooperation with relevant contacts in the federal states is a crucial focus of the regional activities. Regular meetings, participation in local events and lectures are just a few of the services offered.

Operational cooperation with the federal states is carried out through the Administrative CERT Association (VCV). Through the VCV, the CERTs of the federal government and the states improve information exchange in order to react more effectively and quickly to IT attacks. The IT Planning Council has introduced a binding reporting procedure as of 2018 for the exchange of information on cyberattacks, which creates a reporting obligation between the federal government and the states. The BSI provides warnings, situation reports and threat indicators through the CERT-Bund. State contributions to status and incident reports are of fundamental importance and have to be ensured.

THE GOAL: A UNIFORM IT SECURITY LEVEL

Besides the mandate from the Cyber Security Strategy, a decision was also taken at the level of the federal and state interior ministers and senators in 2017 which has major implications for cooperation between the BSI and the states. The need to improve institutionalised cooperation between the federal government and the states in their IT Security efforts was emphasised and the BSI "with

its recognised competence and available resources" was given particular importance.

The underlying goal of better cooperation is the creation of a uniform IT Security level, which becomes more important with regard to the progressive digitalisation of government and the increasing connectivity of IT structures between the federal and state governments. Security consulting and liaison office jointly shape the expansion of the BSI's cooperation with the federal states.

COOPERATION AGREEMENTS WITH THE FEDERAL STATES

Exploratory talks have been held since mid-2017 to identify the states' individual cooperation and support needs and discuss models for implementation. The talks aim to reach concrete agreements that strengthen cooperation. The BSI initiated model partnerships with the states of Hesse and Rhineland-Palatinate in 2017, followed by North Rhine-Westphalia in February 2018. The starting point was the signing of declarations of intent setting out concrete areas of cooperation.

The BSI offers this form of cooperation equally to all federal states, where priorities and support services are adapted individually and according to needs. The establishment and expansion of IT Security structures in the federal states is specifically supported by BSI expertise to strengthen IT Security. The municipalities must also be involved in strengthening cooperation between federal and state governments. They should be connected to the Alliance for Cyber Security from a BSI perspective. Because of the large number of municipalities, it is important to bundle or integrate multipliers when defining interfaces.

WHAT THE BSI HAS TO OFFER

The range of services offered by the BSI was compiled in a product and service portfolio and prepared to meet specific needs (see Fig. 1). Starting from the category "information," which includes standards such as basic IT-Grundschutz as well as status reports and warnings, the provisioning effort increases with each category in accordance with the pyramid shown. Besides "training and education offers" and "cooperation platforms" such as the Alliance for Cyber Security, the BSI also offers "consulting services" on various questions regarding the implementation of IT Security. Due to the high level of resources involved, the BSI can only offer concrete "technical services" such as support or even the "adoption of technical protection measures" on request; in some cases, the corresponding legal prerequisites have yet to be created. Federal authorities as traditional customers of the BSI can currently make use of all of the BSI's services.

In order to achieve a uniform high level of IT Security in federal and state government, the BSI aims to make the same operational support services available to the federal states as are currently available to the federal government. However, there is still no legal framework for this. ■

THE BSI PRODUCT AND SERVICE PORTFOLIO

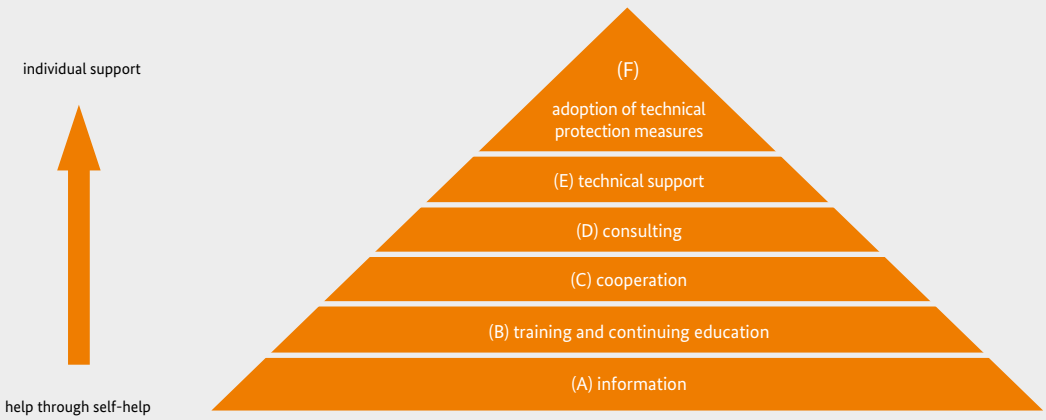


Fig. 1

State Secretary Randolf Stich, Ministry of the Interior and for Sport in Rhineland-Palatinate

Interview with Randolf Stich

"Information Security is more than putting up Firewalls."

How is Rhineland-Palatinate currently positioned in the area of Cyber Security?

The state government of Rhineland-Palatinate takes the current threat posed by cyber attacks very seriously. Ensuring information security in the state administration is therefore an important concern that is also enshrined in the coalition agreement. It includes an already adopted guideline on information security and is currently being further deepened and implemented. The state has also appointed a CISO (Chief Information Security Officer) to coordinate Cyber Security state-wide and to set up an organisation to address the issue.

The CERT (Computer Emergency Response Team) in Rhineland-Palatinate operates the country's central attack detection systems, which detect and fend off more than 20 million security-related events every day. The services are also used by the municipalities and Saarland.

What challenges do you see for your state in this area?

Besides the ever-changing types of threats we face every day, along with targeted attacks on our infrastructure, a major challenge is posed by the shortage of skilled workers. We compete not only with the Federal Government and other states, but also with the economy of the Rhine-Main area for highly sought-after skilled workers.

We have already achieved a high level of security in the centralised areas. However, further expansion into the area is still needed. Information security is as essential for subordinate authorities and services that are not yet centralised as it is for everyone else.

How do you plan to tackle these challenges?

Information security is more than putting up firewalls. We take a holistic approach to information security. Cooperation and the establishment of a security organisation for the whole country are particularly important here. The CISO office has already developed a concept for this.

To counter the existing shortage of skilled workers, we are also taking a cooperative and agile approach. Not every security officer in the state has to reinvent the wheel. But the greatest possible exchange must take place. This also makes it possible to react flexibly and quickly to new threats.

In what areas will you cooperate more closely with the BSI in the future?

We will continue intensifying our work in the CERT network, including the use of an MISP (Malware Information Sharing Platform). We are already making a major contribution to providing information on malware. The BSI specialists want to cooperate more intensively, especially with regard to targeted attacks on authorities in the state. In serious cases, the forces of Rhineland-Palatinate are supported by Mobile Incident Response Teams (MIRTs), special task forces of the BSI for coping with cyber attacks.

What do you feel are the advantages of partnering with the BSI?

Cyber Security is a state-wide challenge that requires cooperation between the federal, state and local governments. Rhineland-Palatinate wants to make its contribution to achieving greater security for everyone involved.

Access to BSI expertise is also of great benefit to us, just as we share our information with the BSI. The mutual exchange is of benefit to both partners.

What partnerships already exist in the field of Cyber Security and how do you evaluate them?

Together with the municipalities, we are working on a comprehensive concept for integrating them into a state-wide Cyber Security strategy. Rhineland-Palatinate is also already cooperating across borders: our CERT is taking over services for the administration of Saarland. We are striving for further cooperation in the future.

As a representative of a state government, how would you like the Federal Government to approach the future of the partnership?

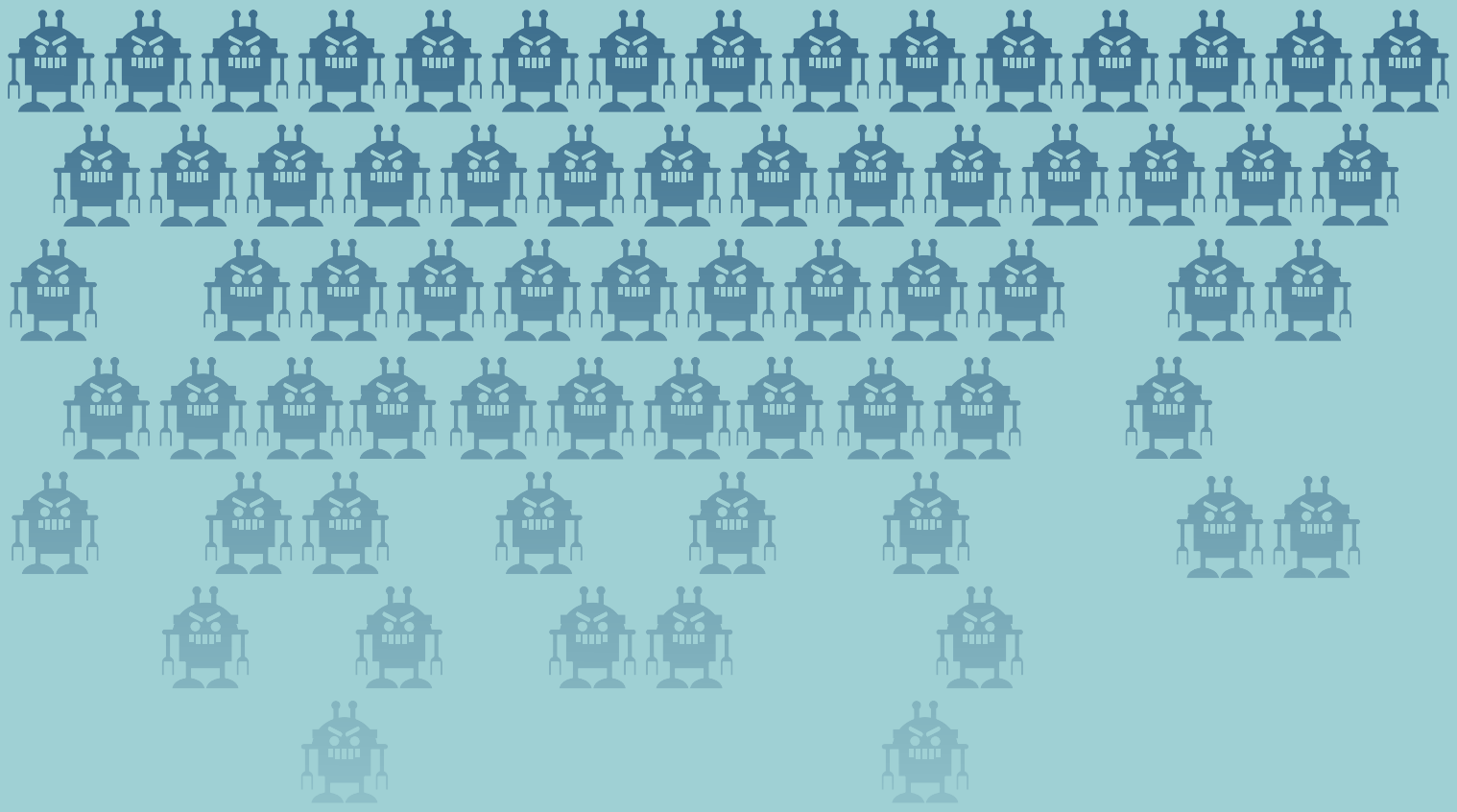
We would like the National Cyber Security authority to grant us access to the products and services currently available that the BSI has so far only provided to the federal administration. But for now, we are happy with how quickly our cooperation with the BSI has started.

IT SECURITY
IN PRACTICE

AVALANCHE SINKHOLING

Many Systems are still Infected

The Police of the German State Lower Saxony – ZKI Lüneburg and the Public Prosecutor's Office in Verden successully unveiled the botnet infrastructure of Avalanche in an international operation with decisive support from the BSI. At that time, the BSI took extensive information and protection measures for affected users. Nevertheless, many systems are still infected today. Citizens should act in their own interest and clean their systems.



It was a spectacular operation spanning a total of 30 countries. It lead to five arrests, 37 house searches and the seizure of 39 servers in several countries – 221 additional servers were shut down by hosting providers. Over 830,000 botnet domains were seized or redirected to so-called sinkhole servers. Victims were found in over 180 countries. It became clear in the end that Avalanche was the largest botnet infrastructure known to date. More than 20 botnet families were identified. An international group of perpetrators had infected hundreds of thousands of private and business computer systems with various types of malware.

CITIZENS MUST ACT

The BSI, which as the National Cyber Security Authority had been instrumental in supporting the operation, placed the protection of citizens first from the outset. By using the sinkhole servers, the malware on infected computers was no longer able to communicate with the originators' servers, removing their control over the malware on infected computers. However, since the IP addresses and the access time of the affected computers were still registered, it was possible to inform the respective internet providers responsible for German IP addresses and the concerned users.

To prevent further virus infections, the BSI provided signatures obtained from the analysis of the detected malware variants to the manufacturers of antivirus software.

About a year after the Avalanche survey, however, in late 2017, analyses of the virus figures showed that a large number of infected systems still existed. While the number in Germany has fallen by 61 percent in only one year, which is great success compared with the worldwide development of a 45-percent reduction, this also means that many affected users have still not cleaned their systems.

There is an urgent need to act. The BSI has therefore extended and enlarged its protection and information measures. Around 4,800 German IP addresses are currently detected as having infected computers and are notified by providers on a daily basis.

HAZARD POTENTIAL

Users with infected computers must assume that the offenders have accessed information stored on the infected computer and, for example, spied out IDs and passwords. Citizens were also deceived in internet banking, ransomware was installed and computers were used to send spam emails. The identified malware was mainly used on Windows computers, in some cases also on Android smartphones, for example to intercept texts. ■

GET ACTIVE FOR YOUR SAKE!

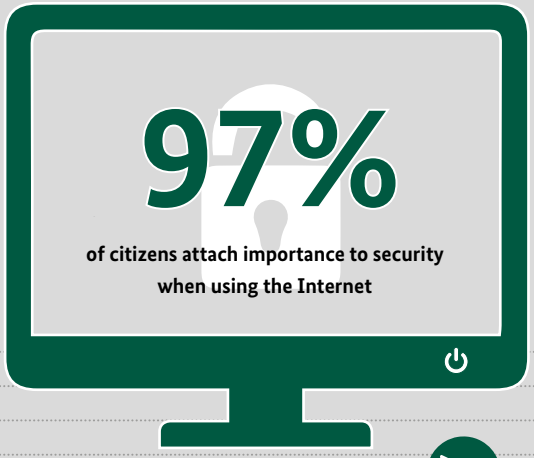
If your provider notifies you that computers connected to your internet connection are infected, you should act immediately. You must assume that the malware has been spying out passwords and credentials. You will find extensive information on how to eliminate the virus infections at www.us-cert.gov/avalanche.

It is important that you change all important passwords immediately after notification and cleaning your computer. Check your bank statements for missing or incorrect posts. You should proceed similarly with all customer accounts, such as online merchants and auction houses, to prevent an unauthorised person from doing business on your behalf.

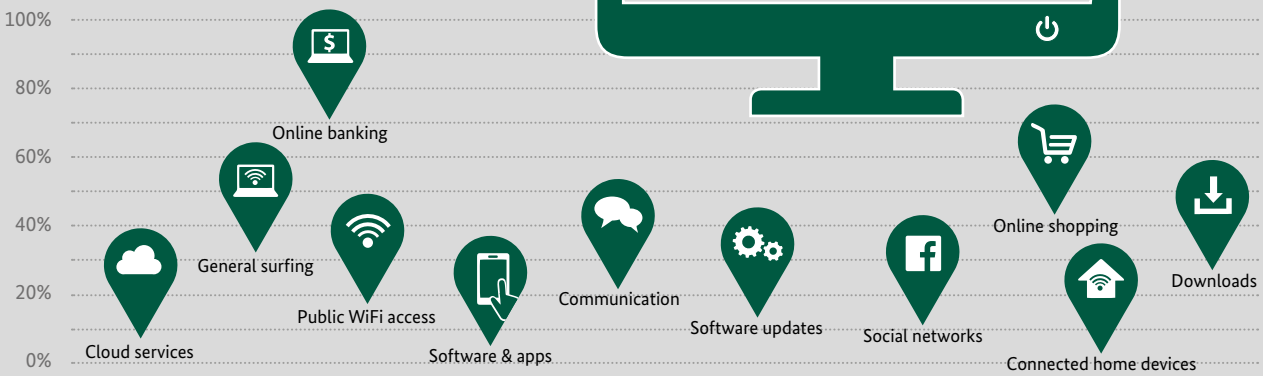
For more information see https://www.bsi-fuer-buerger.de/botnetz

Putting IT Security into Action

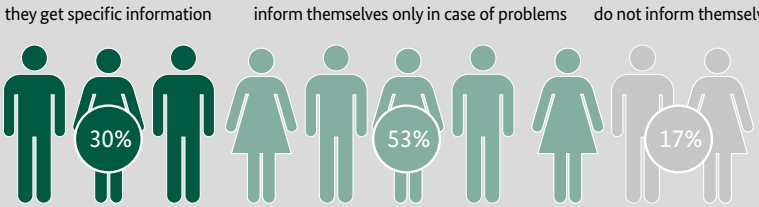
Making digitalisation secure is a central concern of the BSI. But how important is internet security to the German public? How do people protect themselves from online threats? A representative survey from the BSI and the Police Program Crime Prevention of the Federal States and the Federal Government (ProPK) provides answers.

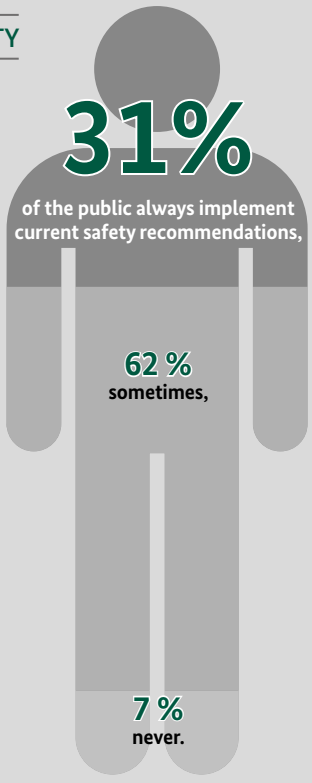


SECURE INTERNET USAGE IS PARTICULARLY IMPORTANT TO RESPONDENTS FOR THESE ACTIVITIES

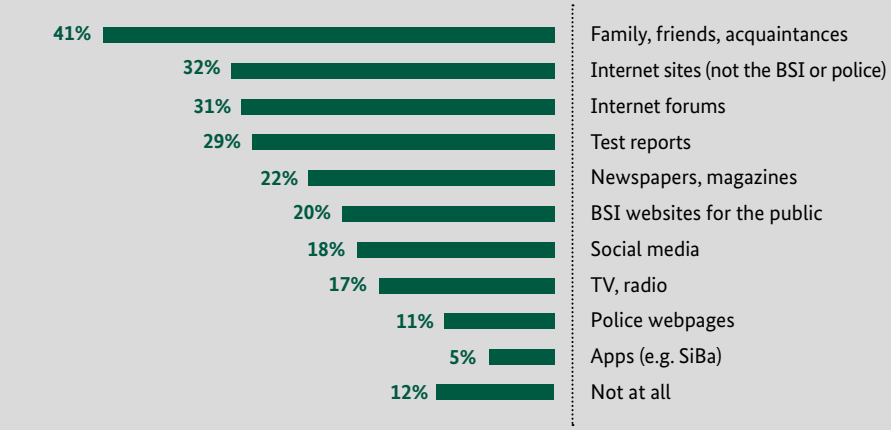


ONE THIRD OF CITIZENS INFORM THEMSELVES SPECIFICALLY ABOUT IT-SECURITY





The public receives information on IT Security from ...



VICTIMS OF INTERNET CRIME

4 of 10 citizens have already fallen victim to cybercrime.

I helped myself.

I asked my family, friends or acquaintances for help.

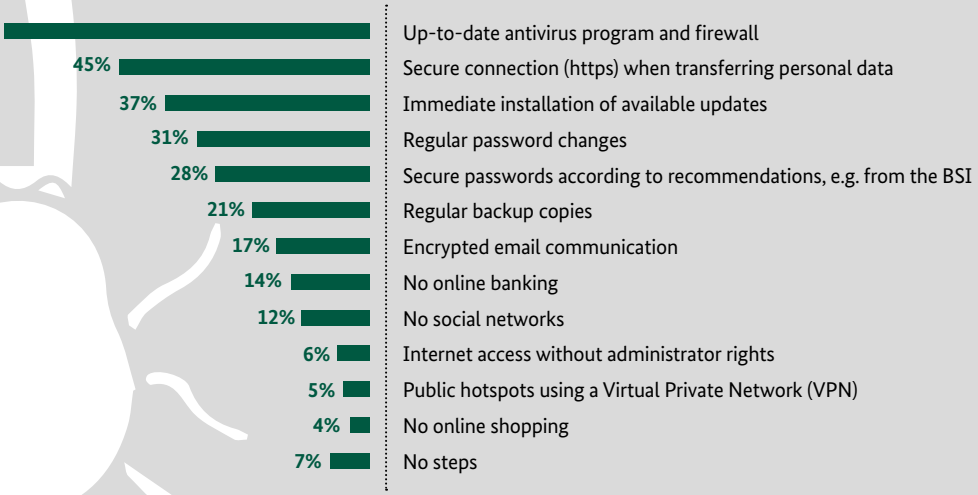
About one in four citizens is not able to identify crimes on the Internet.

6 out of 10 citizens leave the website or delete the email if they suspect crime.

STEPS TO PROTECT FROM THREATS ON THE INTERNET

66%

Two-thirds of citizens use up-to-date antivirus programs and firewalls.



For more information see https://www.bsi.bund.de/Umfrage_Internetsicherheit_2018

Source: Federal Office for Information Security / Police Program Crime Prevention of the Federal States and the Federal Government. Representative online survey of the German-speaking population aged 14 to 66, conducted by Ipsos Public Affairs, survey period 28 September to 9 October 2017, n=2.010

LIVING WITH THE CONSEQUENCES

By Joachim Gutmann, Glücksburg Consulting AG

Lukas Hospital: Armed against Cyber Attacks

More than two years ago, the Lukas municipal hospital in Neuss, Germany (Städtische Kliniken Neuss – Lukaskrankenhaus – GmbH) was shaken by a cyberattack and nearly became the victim of blackmail. Lukas Hospital did not pay, however, but went digital, switching temporarily to diving stations and strengthened its defence mechanisms for cyber attacks – voluntarily and successfully to this day.

"The cyber attack on Ash Wednesday heralded a week-long digital Lent."

Ash Wednesday, 10 February 2016: At 9:00 a.m., the telephones in the IT department of Lukas Hospital start ringing off the hook. Some computers are not starting. Others are displaying a letter written in incorrect English. Many display error messages. The reason: an encryption Trojan hijack from an infected attachment in an email. Its goal: to extort a ransom. All computer data has been encrypted, the letter says, and they now need to write to a certain email address.

EMERGENCY ON ASH WEDNESDAY

But the clinic management decided not to do that. Instead, they called the State Criminal Police Office (LKA) and filed charges. The clinic's technicians shut down all systems and moved the clinic into the pre-digital age. Two days after the attack, the Federal Office for Information Security (BSI) was called in and sent experts to Neuss.

"The cyber attack on Ash Wednesday heralded a week-long digital Lent," recalls Commercial Director Dr. Nicolas Krämer. In order to protect sensitive patient data and prevent the virus from spreading, messengers were used instead of bits, laboratory values were recorded on paper, and people communicated by telephone and not by tablet. Planned major surgeries were postponed, the clinic called off emergency care and stopped admitting seriously injured people.
A blessing in disguise: The backup of the night before was not affected. However, rebooting was tedious and returning to the old IT infrastructure, although at a good level before the crash, did not seem advisable. Instead, a new IT network structure and Citrix technology were used, which are much more secure. "We have introduced a sandbox system to defuse infected email attachments and have entered into a cooperation with a Dutch cyber defence centre, thinking along the lines of 'prevention is better than rehabilitation,'" says Krämer. The technical security steps are accompanied by an awareness campaign for employees. They receive a short video clip on IT Security once a month.

OPERATIONAL AGAIN

More than a month after the attack, the systems were up and running again. The hospital had to spend around one million euros, mainly for external IT

"The step to shut down the IT systems was the only right one. No patient was harmed, no patient data compromised, and the hospital was able to use the crisis as an opportunity."

consulting fees. "But the step to shut down the IT systems was the only right one," the Director is convinced. "No patient was harmed, no patient data compromised, and the hospital was able to use the crisis as an opportunity."

The cyber attack in Neuss has not triggered any doubts about the need to push ahead with digitalisation in the health care system and also at Lucas Hospital. "Progress in the health care system is not possible without digitalisation," says Krämer. "The IBM Watson supercomputer contains the textbook knowledge of all the medical textbooks in the world and will help doctors to make accurate diagnoses in the future. Major advances in cancer research will be achieved through worldwide big data analyses. And in just a few years' time, it will not only be possible to sequence the individual human DNA for one hundred euros, but also to show the probability with which a person will suffer a certain disease at a certain age."

Data security and digitalisation are not poor bedfellows – on the contrary: in principle, digital data is better protected than analogue data, the decision makers in Neuss are convinced. At present, patient data is still transmitted most frequently by fax to general practitioners and is often accessible or visible to unauthorised parties. The legally prescribed 30-year archiving of patient records on paper in inadequately secured warehouses is also a security problem. In contrast, the E-Health Act lays down security standards such as double encryption and data logging access. And the GDPR will regulate how data protection can be combined with the use of large amounts of data from May 2018.

INCREASED SECURITY REQUIREMENTS

Since July 2017, hospitals with at least 30,000 in-patients per year have been regarded as "Critical Infrastructure" and must align their IT infrastructure with the regulations of the IT Security Act. The new rules apply to a total of 110 hospitals and clinics. From the entry into force of the corresponding ordinance in accordance with Section 8b (3) BSIG, they must

- name a contact to the BSI as the central reporting office for IT Security of Critical Infrastructures and report major disruptions to their IT, provided they could have an impact on the availability of critical services;
- prove within two years to the BSI that they have taken appropriate organisational and technical precautions to avoid disruptions of the availability, integrity, authenticity and confidentiality of their IT systems, components or processes that are crucial to functionality;
- regularly prove adherence to IT Security in accordance with the state of the art to the BSI (Section 8a BSIG).

In a first step, hospitals must identify the underlying processes and plan, implement and document appropriate security measures. In a second step, the implementation of the measures must be certified by a suitable testing body. Their audit report is submitted to the BSI every two years with details of the audited Critical Infrastructure and the contact.

If security deficiencies are discovered, the BSI may, in agreement with the supervisory authorities, order their elimination and, if necessary, also oblige the manufacturers of the corresponding IT products and systems to cooperate in accordance with Section

8b BSIG. Conversely, the BSI must collect and evaluate all information relevant for the defence from attacks on IT Security Critical Infrastructures and pass it on to the operators and the competent (supervisory) authorities.

ANYONE CAN BE ATTACKED

Lukas Hospital in Neuss is not one of the institutions covered by IT Security law. According to the German Hospital Association, only about ten percent of all clinics reach the limit of at least 30,000 in-patients per year. These large facilities have always invested heavily in IT Security and usually have their own emergency plans. The Marburger Bund recently criticised the fact that smaller institutions were not taken into account, given that the policy "cannot be reconciled with the reality of supply."

In 2013, the BSI also published a risk analysis entitled "Hospital IT." It came to the conclusion that the IT Security situation of hospitals differs widely: "While large hospitals, especially university clinics, are aware of the importance of the issue," it reported, "smaller hospitals in rural areas in particular tend to treat it with subordinate priority due to a lack of budget and personnel."

This could have fatal consequences, as the threat is real and even random attacks can cause considerable damage. The massive attacks with the blackmail software Wannacry and Petya in 2017 showed this once again. That time, they hit hospitals in the UK and the US. But as they know in Neuss: "The attack has made it clear to us that cyber attacks can affect anyone, not just the big players," summarises Krämer. "And that's why everyone should protect themselves to the best of their ability." ■

Joachim Gutmann is a freelance journalist. He works for Glücksburg Consulting AG as a communications expert.

DIGITAL SOCIETY

BLOCKCHAINS IN USE

By Dr. Christian Berghoff and Dr. Ute Gebhardt, Section Technological Principles of Secure Electronic Identities, Chip Security

Appropriate Application Models for Suitable Security Goals

Companies continue to show great interest in blockchains and their applications. The German coalition agreement also announces this technology will be tested. When designing solutions, however, one should be aware that the selected blockchain model must be suitable for the intended application and the desired security goals.

Blockchains implement a technology for distributed data storage (cf. BSI Magazine 02/2017). New data blocks are attached to a constantly growing chain and linked to their predecessors by a cryptographic hash function. The resulting blockchain is distributed in a decentralised peer-to-peer network. A so-called consensus mechanism ensures agreement among network nodes about which data to commit and consistency of this data.

The choice of this mechanism has a direct impact on the scalability of the blockchain. The well-known "proof-of-work" approach, used for instance by the popular cryptocurrency Bitcoin, allows only for a low data throughput and is extremely energy-intensive as well.

Significantly more efficient message-based methods can be used in private or permissioned blockchains, which – unlike public unpermissioned blockchains such as Bitcoin – do not endow all users with the same access rights. Due to these restrictions, they are also less problematic in IT Security and legal matters. The choice of a suitable blockchain model is thus important, and beyond cryptocurrencies, in practice most applications are based on private blockchains.

DEPLOYMENT SCENARIOS

The majority of blockchain applications are based on one of the following concepts:
Firstly, they can record the transfer of ownership of assets. In this way, one expects to securely settle transactions without relying on a central authority. Use cases include cryptocurrencies, above all Bitcoin, but also pilot projects in the energy sector for instance. In the event of transport bottlenecks in the power grid, one of them stores the surplus energy in a large number of batteries distributed over a given area and releases it again once the situation has normalised. Accounting data is recorded in a blockchain.

Designing a Secure Blockchain – Key Points of the BSI

By Dr. Manfred Lochter and Dr. Sarah Maßberg, Section Requirements for and Development of Cryptographic Mechanisms

For the BSI as Germany's National Cyber Security Authority technical and design aspects of blockchain with regard to IT Security are in the foreground. Five key points were published by the BSI in February 2018 and presented at an event in the series "The BSI in Dialogue." Another event is planned for late-2018 with a special focus on the financial sector. The key points are to raise awareness of the challenges of IT Security in blockchains and to stimulate dialogue with business, science and administration.

The BSI sees the following core statements as key points in its approach to "Blockchain and IT Security":

Blockchain alone does not solve IT Security problems

The target characteristics of blockchain such as immutability, traceability and decentralisation, as well as its strong cryptographic foundation can generally have a positive effect on the security features of IT solutions, but at the same time the security of the hardware and software used and the underlying protocols must be ensured. The security of the blockchain's external interfaces must also be taken into account, especially for authentic data insertion or readout. For many applications using blockchains a trusted central authority will still be necessary.

Choosing the right blockchain model is important

Depending on the application, a suitable consensus mechanism must be selected to reach agreement on the correct state of the blockchain. In addition, access to the network (unpermissioned – permissioned) as well as access to data (public – private) and general role and rights management can be individually defined. The "unpermissioned public" blockchain with "proof-of-work" consensus used by Bitcoin is unsuitable for many applications.

Other applications plan to use the technology for ensuring the integrity of documents by storing their electronic fingerprints (hash values) into a blockchain. The integrity of a document may later be verified by comparing its hash value to the stored one. Decentralised access options are expected to increase efficiency in integrity assurance and reduce redundant structures. This use case is implemented by a solution that manages digital certificates for instance.

Further applications intend to use blockchains to control business processes by storing intermediate steps in data blocks. The transparency and immutability of blockchains ensure a verifiable, tamper-proof record of process steps. Supply chain tracking in global trade offers a prime example of this use case.

TRUST MODEL

Since the advent of blockchain technology with Bitcoin, its proponents assert it can get by without any reliance on intermediaries and relies solely on cryptographic proofs. A certain amount of trust in several parties is however still required. In the case of cryptocurrencies, these include mining pools that theoretically can manipulate the blockchain, as well as exchanges in which bitcoins are traded for currencies such as euro and U. S. dollar. Even if they behave honestly themselves, they are attractive targets for attackers, and users must trust them for their appropriate protection. The same applies to the implementation security of digital wallets. The programmers of the blockchain software in use hold an important position of power – which is true even for open source projects.

This rather vague trust model of public blockchains is in contrast to the hierarchical model of private blockchains, in particular private permissioned blockchains. These are similar to traditional solutions – e.g. based on databases – insofar as users have to place stronger trust in the owners of certain roles.

ASSESSMENT OF FEATURES

When equipped with appropriate cryptographic algorithms, blockchains can ensure integrity and availability. Due to their inherent transparency, however, confidentiality is a demanding goal. As a rule, authenticity must also be achieved via additional measures.

In the construction of blockchains, security aspects must be considered at an early stage

In accordance with the intended security objectives, aspects such as confidentiality, integrity and authenticity of transaction data, secure execution of smart contracts and user identity management must be appropriately modelled and implemented in the blockchain. Confidentiality is a particularly demanding goal in blockchain applications. Selecting algorithms and protocols should follow BSI's guidelines.

Sensitive data with long-term protection needs must be specially protected in a blockchain

Due to the long availability (with simultaneously potentially high sensitivity) of data in a blockchain, achieving long-term security poses a particular challenge. It is important to ensure that the security mechanisms of the blockchain can be exchanged if necessary. In particular, requirements arising from the threat posed by potential quantum computers and technical advances in cryptanalysis must be taken into account.

Uniform security levels for blockchains must be defined and enforced

The standardisation of blockchains needs to be further pursued, taking appropriate account of IT Security aspects. A security certification of selected components according to generally accepted criteria can be useful for certain applications. Blockchains operated transnationally require international coordination. The BSI will continue to monitor and assess the development of the blockchain technology and, within its remit, will contribute to the development of recommendations and requirements for blockchain security mechanisms.

When designing solutions, the desired security requirements must be analysed at an early stage and one has to check whether the security features of the selected blockchain model satisfy these requirements. For example, transparency can be decisive for the documentation of business processes, whereas a lack of confidentiality is unacceptable when storing sensitive data. Decentralisation is worth considering when there are no trustworthy instances. In case these exist, however, private blockchains with their hierarchical trust model and their markedly higher efficiency may be preferable.

In order to decide how the desired functionality can be implemented most reasonably, a comparison to existing technologies is also advisable. Compared to databases, blockchains offer intrinsic advantages in terms of availability and transparency and require less trust in a central authority. In terms of confidentiality and processing speed, significant disadvantages are manifest. ■

These points can also be found in the paper "Designing a secure blockchain – Key points of the BSI" at https://www.bsi.bund.de/Blockchain-Eckpunktepapier

Data Security for Connected Mobility

By Dr. Joachim Damasky, VDA Managing Director

The Car is not a Smartphone

The German automotive industry is driving the development of networked vehicles to ensure safety, comfort and environmental friendliness. of the vehicles. But the car is not a smartphone.

Dr. Joachim Damasky, VDA Managing Director

The German automotive industry is driving forward the development of connected vehicles to further improve vehicle safety, comfort and environmental friendliness. But the car is not a smartphone: vehicles need much higher security standards than tablets or mobile phones. Protecting customers and their data in the vehicle is particularly critical. On the one hand, vehicle connectivity enables new applications for customers, but on the other hand, this development could make the vehicle vulnerable to cyber-attacks. A vehicle's safety is highly relevant to its user. The integrity and safety of the vehicle and driver therefore have top priority and must be guaranteed at all times.

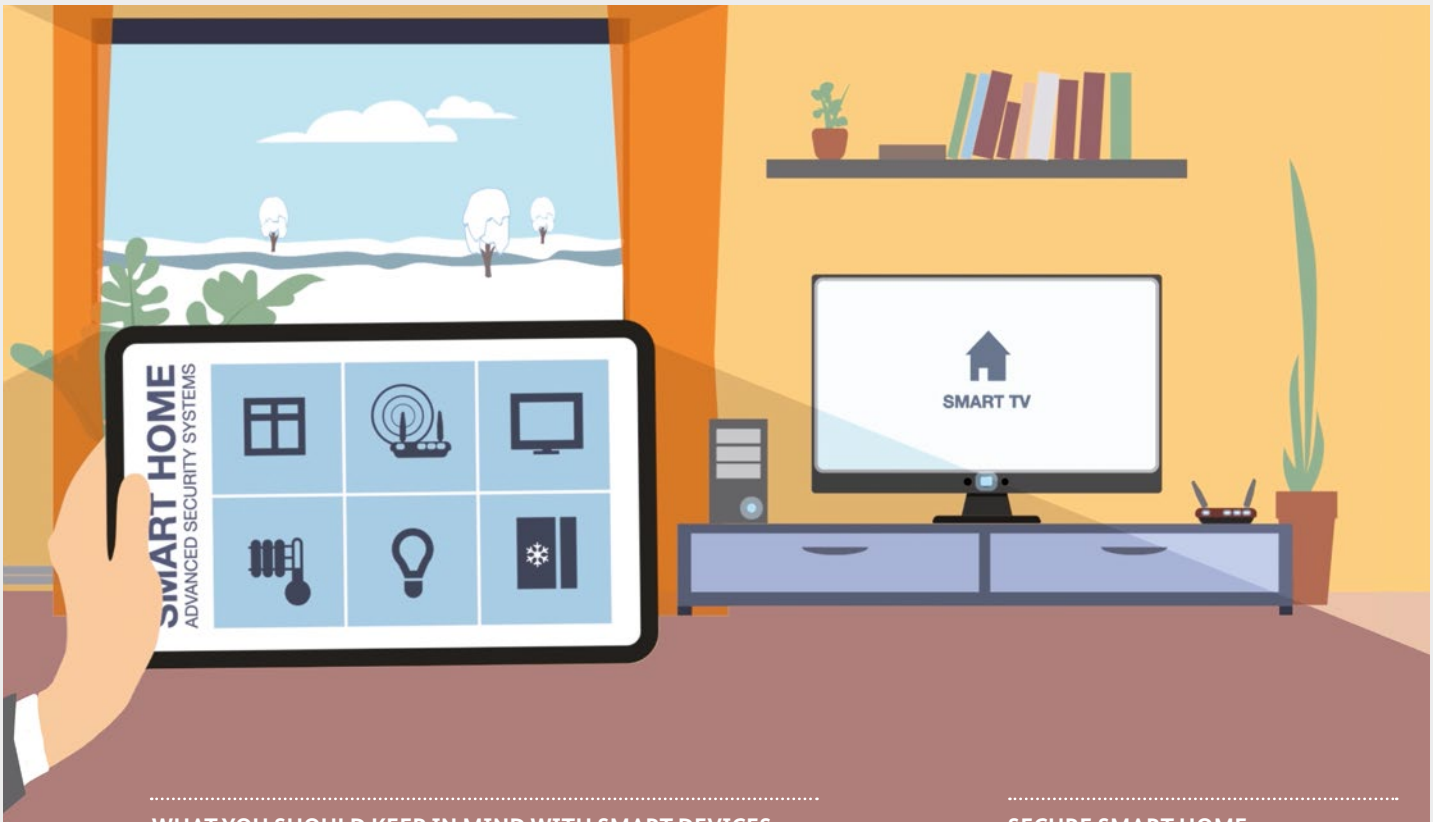
The German automotive industry has recognised the demands on vehicle safety and is investing in the protection of its products to meet them accordingly. A uniform methodical procedure for the development of vehicle systems and their connectivity is described and applied in industry to ensure a high level of security protection for new products.

With "NEVADA – Share & Secure," the German automotive industry has developed a concept that enables the secure transmission of data generated in the vehicle and makes it usable for public authorities and industry. This will help further improve road safety and support the development of digital innovations and new business models. Public authorities such as fire departments and police can use data generated in vehicles to significantly increase road safety. Evaluating vehicle data in conjunction with traffic infrastructure data can identify traffic jams as they occur, locate icy streets more efficiently or detect accidents. Infrastructure data must, however, be provided by public authorities. The multitude of possibilities that analysis offers is a decisive added value for the future safety of our roads. ■

Smart Home

Basic Tip from the BSI

From smart TVs and refrigerators to remote-controlled heaters and security cameras, the connected home, where every device can be monitored and controlled from a smartphone or tablet, is no longer science fiction. If you want to benefit from the possibilities of a smart home, aware of and untroubled by risks, consider these simple instructions and steps. Protect your smart home from cybercriminal attacks.



WHAT YOU SHOULD KEEP IN MIND WITH SMART DEVICES:

- Devices should support encrypted communication.
- Vendors should provide software updates and close security holes for as long of a period as possible.
- Devices should be able to be used locally without cloud or internet connection.
- Check how manufacturers handle collected usage data.
- Replace preset passwords with secure, individualised ones.

SECURE SMART HOME

Connecting devices to the Internet is only recommended if external access is absolutely necessary for its function. Devices can often sufficiently operate within a home network. Mobile devices should also control the home network from a virtual private network (VPN).

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

Consumers in the Digital World

By Hanna Heuer, Section Cyber Security for Citizens; Public Relations, Florian Schumacher, Section Cyber Security for Society and Helga Zander-Hayat, Head of Market & Law and Member of the Executive Board, Consumer Association of North-Rhine Westphalia (Verbraucherzentrale NRW e. V.)

One Year of Cooperation Between BSI and the Consumer Association of North-Rhine Westphalia

The Consumer Association of North-Rhine Westphalia and the BSI look back on a successful first year of cooperation. In the future, the joint work on a wide range of topics is to be continued and further expanded.

On 1 March 2017, the Executive Director of the Consumer Association of NRW Wolfgang Schuldzinski and President of the BSI Arne Schönbohm signed a Memorandum of Understanding to increase Information Security for consumers. The goal was to work together on concrete information security issues, in order to benefit from the mutual expertise and legal competencies.

CONSUMERS IN THE DIGITAL WORLD

Thanks to the ever-increasing connectivity, more and more our daily lives are inseparably intertwined with the digital world. The latest fashionable clothes are ordered over the Internet, transfers are made on a smartphone, the smart home is controlled via an app and vital data is digitalised with a tracker. In many situations, this development facilitates our daily activities and opens up new opportunities. Nevertheless, it also comes along with risks, above all concerning Cyber Security. This requires resilient consumers operating in a secure infrastructure and with the ability to act competently. It is clear that the protection of consumers and a cyber-secure environment are a prerequisite, if digitalisation is to succeed.

TOPICS IN THE FIRST YEAR OF COOPERATION

In order to counter threats and jointly contribute to a rise of Information Security, the Consumer Association of NRW and the BSI agreed to cooperate over the past year. The combination of mutual competence has already proven very fruitful in its first year. This is evident from the following four examples of collaboration:

1

UPDATE CAPABILITY OF SMARTPHONES

Smartphones with an outdated operating system are being retailed as new, but no security updates are provided by the manufacturer anymore. This results in some serious security issues while using them. One example are the vulnerabilities that became known in July 2015 under the name “Stagefright”, in the eponymous multimedia framework of Google’s Android operating system. How to update software along with missing update possibilities is not easy to detect for most consumers. But transparent information is necessary for an informed purchase decision. However, that is often insufficiently supplied by vendors. After the BSI conducted a technical examination and identified vulnerabilities on a smartphone, the Consumer Association of NRW used its competence and initiated legal action against the seller of the device concerned, because of insufficient consumer information. The case is ongoing.

2

PHISHING-RADAR

Fraudsters use phishing messages on counterfeit pages to try to persuade users to reveal their access data, for example for online banking. The Consumer Association of NRW has collected information on internet fraud since 2010. Consumers can send fraudulent emails directly to an email address, set up for this purpose (phishing@verbraucherzentrale.nrw). The long-term findings are now being exchanged with the BSI and contributing to the assessment of the state of IT Security.

3

JOINT EDITORIAL OFFICE FOR CONSUMER PROTECTION AGENCIES

Information and awareness-raising activities make an important contribution to improving user proficiency. The BSI has an established offer in this regard with "BSI for Citizens." The Consumer Protection Agencies are well-known contact points on the Internet and in the nationwide counselling centres. Website contents are produced by a central joint editorial office affiliated with the Consumer Protection Agency in NRW. BSI's technical expertise can be incorporated into this work so that consumers can find out more about cyber security issues online.

4

CONNECTED TOYS

Connectivity has even found its way into the children's room. More and more toys have direct or indirect interfaces to the Internet. Aspects of data protection and data security are therefore becoming more relevant for this product category. In cooperation with the Consumer Association of NRW, the BSI is investigating the safety of connected toys, examining a toy robot for weak points in data security. The robot is controlled via an app over WiFi and works with face recognition technology. It is supposed to be able to interact with a playing child and constantly film its surroundings.

CONCLUSION & OUTLOOK

The Consumer Association of NRW and the BSI can look back on a successful year of cooperation. The judicial review of the information obligations of retailers with smartphones that do not have an update capability could have a wide-ranging impact. This could result in additional questions and need for action. In other fields, too, both partners want to continue to bring their cooperation to life to jointly increase information security for consumers. This includes the security of hardware and software in the smart home as well as the consumer-relevant issues surrounding the activation of private WiFi hotspots. And of course, security holes will certainly always be on the agenda. ■

AND FINALLY

EVENTS CALENDAR 2018/19

CeBIT

11th - 15th June 2018 in Hanover

The BSI will be on exhibit at CeBIT again in 2018, which will take place in June this year with a new concept for the first time. Under the title "Europe's Business Festival for Innovation and Digitalisation," Messe Hannover is planning a trio of exhibition, conference and festival. The theme of the "new CeBIT" is the digitalisation of business, government and society.

Free and Open Source Software Conference (FrOSCon)

25th - 26th August 20182018 in Sankt Augustin

The BSI will attend the Free and Open Source Software Conference (FrOSCon) 2018, taking place 25-26 August 2018 in Sankt Augustin. The computer science department of the University of Applied Sciences Bonn-Rhein-Sieg is organizing an interesting program with lectures and workshops for free software developers and users, supported by FrOSCon e. V. Trade fair visitors can discover more about several BSI projects in the area of free software at the BSI's project booths.

IFA 2018

31th August - 5th September 2018 in Berlin

The BSI will be on the ground at the Internationale Funkausstellung Berlin in early September. More than 1,800 exhibitors will gather at the world's leading consumer electronics and home appliance exhibition to present their latest product highlights over 159,000 square meters of event space.

it-sa

9th - 11th October 2018 in Nuremberg

In October 2018, the BSI will have a booth and give various presentations at it-sa in Nuremberg. it-sa is the only IT Security trade fair in the German-speaking region and one of the most important in the world. The BSI works together with the German Association for Information Technology, Telecommunications and New Media (Bitkom e. V.) as the spiritual sponsor of the fair. The symposium "Administration integrates secure information technology (ViS!T)" will take place for the first time at it-sa in 2018, to which the BSI is inviting this year. On 8 and 9 October, experts from Germany, Austria, Switzerland and Luxembourg will discuss current challenges in designing processes securely.

16th German IT Security Congress

19th - 23rd May 2019 in Bonn / Bad Godesberg

The BSI is once again organising the German IT Security Congress in May 2019 that will be held in Bonn. With more than 600 specialists in attendance, the biennial congress is a fixture on the calendar for the IT Security industry. Over three days, participants will discuss the state of national and international IT Security developments. The congress aims to shed light on IT Security from different perspectives and to present and develop solutions. The program of lectures is supplemented by an accompanying exhibition.

The call for papers begins in May 2018 when BSI specialists will request submissions for presentation topics. An advisory board will examine submissions and decide which topics will be presented at the 16th German IT Security Congress. More information will be available from May at **www.bsi.bund.de/sicherheitskongress** or by email at **papers2019@bsi.bund.de**.

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

Order your BSI Magazine!

Federal Office for Information Security

Federal Office for Information Security (BSI)
Division Cyber Security for Citizens; Public Relations

P.O. Box 20063
53133 Bonn, Germany
Phone: +49 (0) 228 99 9582 0
Fax: 0228 99 9582-5455
Email: bsi-magazin@bsi.bund.de

Twice a year, the BSI Magazine "Security in focus" offers insights into national and international cyber security, digital society and IT Security in practice. You can receive the latest issues by mail following the Hannover Messe in April and the it-sa in October by subscribing to the distribution list using the form below.

Select what BSI publications you would like to subscribe to:

☐ The BSI magazine "Security in focus" (2/year, print)
☐ The State of IT Security in Germany (1/year, print)

Consent to the storage of your contact data

Last name, first name .....

Organisation .....

Address .....

Zip code, city .....

Email .....

Just send in the form by fax or email:
Fax: 0228 99 9582-5455 | Email: bsi-magazin@bsi.bund.de

Or register directly online:
https://www.bsi.bund.de/DE/Publikationen/BSI-Magazin/BSI-Magazin_node.html

If you wish to revoke your consent to the storage of your personal data and no longer wish to receive BSI publications, simply send us an email at **bsi-magazin@bsi.bund.de**. Your data will be deleted immediately.

Follow the BSI on Facebook and Twitter!
www.facebook.com/bsi.fuer.buerger | twitter.com/bsi_presse
For more information, checklists and tips on cyber security, see
www.bsi.bund.de | www.bsi-fuer-buerger.de | www.allianz-fuer-cybersicherheit.de

Data protection notice: Your personal data will be electronically stored, processed and used in accordance with the Federal Data Protection Act and the EU General Data Protection Regulation. The BSI is responsible for this data and its processing. The data will only be passed on to third parties for shipping purposes. It will not be used for other purposes without your consent.

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:	April 2018
Content and editing:	Stephan Kohzer, Nora Basting and Mark Schulz, 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 18/707-1e
Image credits:	Title/p. 25: GettyImages©enot-poloskun, GettyImages©FredFroese, GettyImages©Guido Mieth Moment, GettyImages©yoh4nn; p. 2: Stephan Kohzer/BSI; p. 4: Bundesministerium des Innern (top), Mesago/Thomas Geiger (below); p. 5: Fink & Fuchs, iStock.com/Grafissimo; iStock.com/Krasyuk (top left), BSI (top right), GSMA (below); p. 6: NCSC; p. 9: NCSC; p. 10: NürnbergMesse it-sa; p. 12: GettyImages©Talaj; p. 14/15: GettyImages©Mehau Kulyk/Science Foto Library; p. 16/17: GettyImages©Dong Wenjie; BSI, GettyImages©3alexd; p. 18-21: GettyImages©Andrzej Wojcicki, GettyImages©PeopleImages; p. 22: GettyImages©bubaone; p. 23: BSI; p. 27: GettyImages©akindo; p. 31: Anapur AG; p. 33: Robert Bosch GmbH; p. 35: BSI; S. 37: BSI (top left), BSI (below left), Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen (right); p.39: Ministerium des Innern und für Sport Rheinland-Pfalz; p. 40, 42, 43: R. Winkler; p. 44-47: Städtische Kliniken Neuss - Lukaskrankenhaus - GmbH; p. 48, 50/51: GettyImages©a-r-t-i-s-t; p. 52: ©VDA 2018; p. 53: junge meister GmbH; p. 54, 55: R. Winkler; p. 56, 57: GettyImages©Ragnar Schmuck

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/BSI-Magazin

www.bsi.bund.de