Federal Office
for Information Security

BSI Magazine 2020/02

Security in focus

Cyber Security in Healthcare

CYBER SECURITY

New Method: Approval of BSI-Certified Products

THE BSI

30 Years of the BSI: Looking Back and Taking a Step Forward

DIGITAL SOCIETY

Actively Designing the New Normal

EDITORIAL

The Year of Exceptions

The corona pandemic is omnipresent and will have a lasting impact. It shows us the fundamental importance of our health every day anew. At the same time, the pandemic has accelerated economic, social and transformation processes and is providing an unprecedented surge in digitalisation in Germany and worldwide.

In this respect, the question of a high-quality, sustainable healthcare system is also becoming increasingly important. The digitalisation of the healthcare system holds enormous potential for a sustained improvement in the quality of medical care: Hospitals, doctors' practices and, above all, patients clearly benefit from digital technologies and better networking and can then offer or take advantage of innovative treatment and care options. Digitalisation in the healthcare sector also poses a whole range of challenges, however. One thing is clear: it cannot succeed without information security. This issue of the BSI Magazine is dedicated to the main topic of Cyber Security in healthcare and presents the BSI's latest approaches in this area. As the central competence centre for information security in Germany, the BSI is also shaping secure digitalisation in this field that is so important for society.

In this issue, we would also like to take the occasion of the 30th anniversary of the BSI to take a look back. Since it was founded on 1 January 1991, the BSI has focussed on the management of IT threats and IT security risks. Due to the constant increase in its tasks and its expansion to address today's three target audiences, government, business and society, it has developed into the central Federal Cyber Security Authority and the central hub for Germany's cyber security architecture.

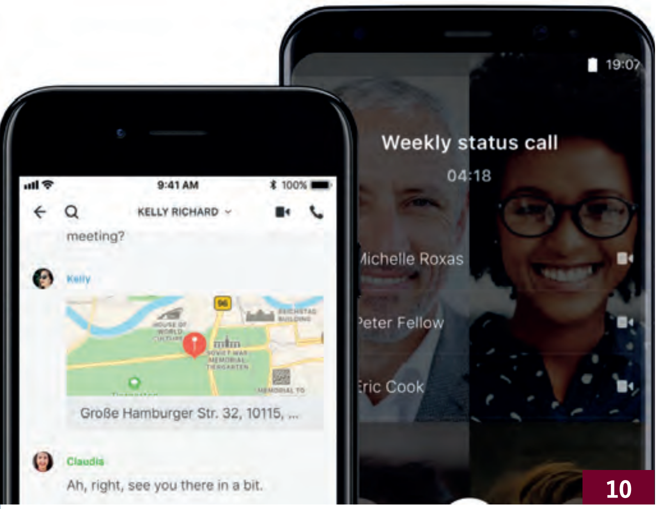
The BSI's expertise is particularly in demand in times of progressive digitalisation because information security and digitalisation are inseparable: They are two sides of the same coin. The BSI stands for both because it shows how information security can function as a new quality feature of digitalisation "Made in Germany."

I wish you pleasant reading.

Sincerely Yours,

Arne Schönbohm

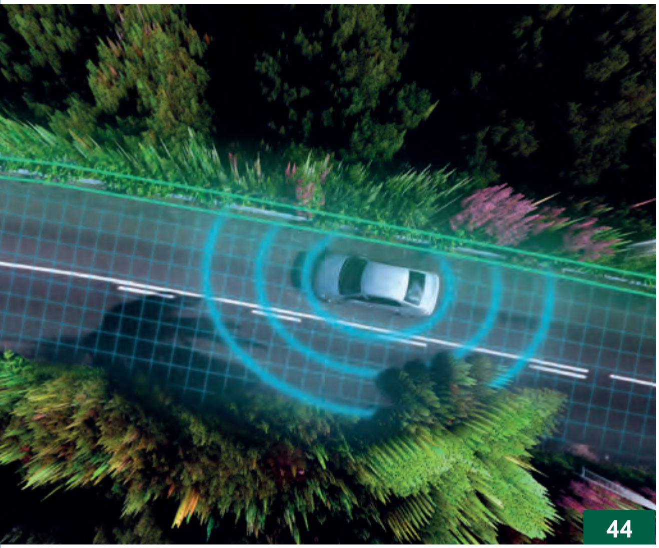
Arne Schönbohm
President of the Federal Office for Information Security



10

20

24



44

54

TABLE OF CONTENTS

NEWS

CYBER SECURITY

THE BSI IN HEALTHCARE

THE BSI

IT SECURITY IN PRACTICE

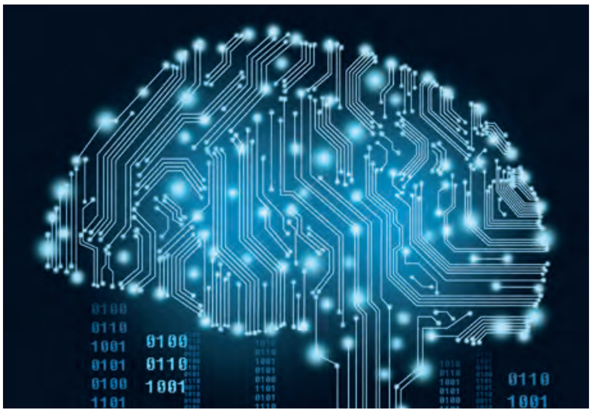
DIGITAL SOCIETY

NEWS

BSI FÜR BÜRGER

BSI Now Has Its Own Podcast: Update Available

The BSI's new podcast is entitled "Update available." It provides listeners with interesting facts about cyber incidents and the latest innovations, bizarre facts and, of course, information about the most important updates for half an hour at the end of each month. The moderator team takes an objective look at the events from the world of networks, technology and cybercrime of the previous four weeks. In each issue, the two journalists Ute Lange and Michael Münz talk about events or questions that have been of particular concern to them. They discuss current events, talk about their fears and explain the background. Those who don't want to get lost in complicated articles can now listen to the most important news on IT security in "Update available." New episodes will always be available for free on Spotify, Deezer, iTunes, Google Podcasts and Youtube.



COMPETITION

SUCCESSFUL in the CHES Challenge

The International Association for Cryptologic Research organised the CHES Challenge again this year as part of the CHES (Cryptographic Hardware and Embedded Systems). The main objective of this cryptographic competition was to attack hidden cryptographic implementations through side channels. This year's team from the BSI was comprised of eight employees from the departments Information Assurance Technology and IT Management as well as Technical Centres of Excellence and won all the prizes awarded in the challenge. CHES is the world's largest and most renowned hardware-related cryptography conference. The annual CHES Challenges are quite prestigious.

#CYBERCONFERENCE2020

EU Council Presidency: Conference A Complete Success

On 9 November 2020, the conference jointly organized by the Federal Ministry of the Interior, Building and Community and the EU Cyber Security Conference was held at the Federal Office for Information Security – due to corona in hybrid format. The expert audience from the authorities of the member states and EU institutions discussed strategic questions and current legislative projects related to European Cyber Security policy in three forums, European cooperation in the response to cross-border Cyber Security incidents, and ensuring security in the area of the Internet of Things (IoT). In addition, the President of the BSI Arne Schönbohm gave interviews on the current threat situation and the role of the BSI, and together with Juhan Lepassaar, Executive Director of the European Union Agency for Cyber Security (ENISA), on the role of ENISA in the European Certification Process for Cyber Security.

IT-GRUNDSCHUTZ

Cyber Security on Board – IT-Grundschutz for Ships under the German Flag

Resolution MSC.428(98) requires the signatory states of the International Maritime Organization (IMO) to adequately address cyber risks from 2021 on. This is to be done within the framework of the prescribed Safety Management System (SMS) in maritime companies and in dealing with safety-relevant events (ISPS Code) on board. In preparation for this, the BSI has already initiated a process aimed at improving Cyber Security in maritime shipping together with various maritime stakeholders since the beginning of 2018. The two “IT-Grundschutz Profiles for Shipping Companies” – Shore Operation (2018) and Ship Operation (early 2020) – have resulted from this collaboration.

Based on this, the BSI and the two authorities responsible for ships under German flag, the Berufsgenossenschaft Verkehrswirtschaft Post-Logistik Telekommunikation (BG Verkehr) and the Federal Maritime and Hydrographic Agency (BSH), have now published the working paper “SM CYBER SECURITY 2020.” The previous recommendation of the BG Verkehr concerning the implementation of the SMS has been extended to include aspects of information security in accordance with IT-Grundschutz and supplemented with practical implementation instructions from the IT-Grundschutz profiles and the ISPS Code. Thus all common requirements (such as risk analysis) have been consolidated and united in the established methodology (SMS), in order to minimise effort for users from the shipping companies and to avoid duplication.

CYBER SECURITY

Safely Surviving the Crisis with IT-Grundschutz

New BSI Standard 200-4: Business Continuity Management

By Cäcilia Jung and Daniel Gilles, Section BSI Standards and IT-Grundschutz

The initial effects of the COVID-19 pandemic in the spring of this year have confronted nearly all institutions with the challenge of maintaining their business operations under difficult conditions. An emergency management system or Business Continuity Management System (BCMS) is the tool of choice for this purpose. The updated BSI Standard 200-4 provides institutions with practical and adaptable instructions for setting up and permanently operating a BCMS.

If a crisis or emergency occurs in an institution, action usually needs to be taken immediately. Human lives must be saved, incidents contained, alternative suppliers found and business operations "somehow" continued in order for an institution to survive an incident.

If no precautions have been taken in advance, solutions must be found as quickly as possible during the crisis. The structures in normal business operations, or AAO for short, often have decision paths that are too long to be able to react adequately and avert situations that threaten the institution's existence. To avoid this, a staff structure (Special Organisational Structure) is established in BCM so that the institution can react and make decisions even in an emergency.

OVERVIEW OF EMERGENCY MANAGEMENT

In addition to the Special Organisational Structure, a BCM for the most time-critical processes creates all the prerequisites for a planned emergency operation in case of an emergency, thus ensuring the existence of the institution. To this end, plans are drawn up in advance and continuity solutions implemented to compensate for the loss of resources (e. g. employees, buildings or IT). The staff coordinates the activities to get into emergency operation and continue it until normal operation is possible again. Figure 1 shows an example of how a damage event can be managed in different phases with the help of a BAO and corresponding emergency plans including continuity solutions. Further details can be taken from the descriptions in the BSI Standard 200-4, chapter 2.3 "Procedure for Managing an Emergency":

SYNERGY POSSIBILITIES

In contrast to the BSI Standard 100-4, the BSI Standard 200-4 shows numerous synergy possibilities with related topics and management systems in the areas of IT security (and in particular the BSI Standard 200-X series), IT service continuity and outsourcing. This allows for resources to be bundled across the various disciplines. The BSI Standard 200-4 can be used alone or in combination with the BSI Standard 200-x series.

STAGE MODEL

In order to meet the requirements of large corporations, medium-sized companies and public authorities, the BSI

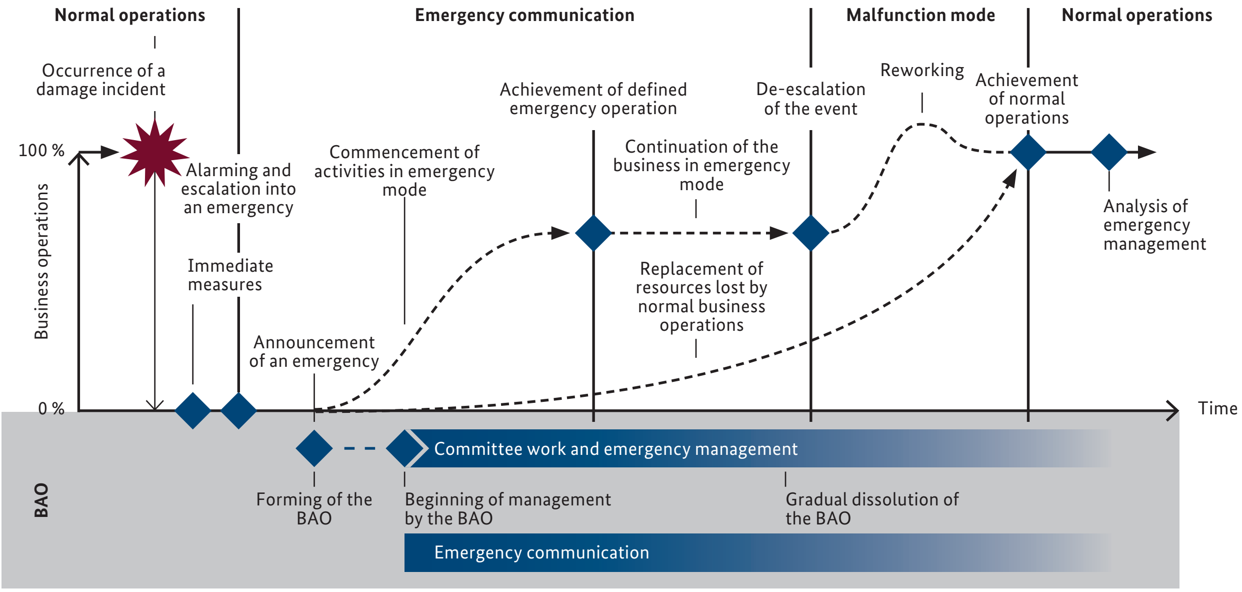

Normal operations
Emergency communication
Malfunction mode
Normal operations
Occurrence of a damage incident
Achievement of defined emergency operation
De-escalation of the event
Reworking
Achievement of normal operations
100 %
Alarming and escalation into an emergency
Commencement of activities in emergency mode
Continuation of the business in emergency mode
Analysis of emergency management
Business operations
Immediate measures
Replacement of resources lost by normal business operations
Announcement of an emergency
0 %
Time
Committee work and emergency management
BAO
Forming of the BAO
Beginning of management by the BAO
Gradual dissolution of the BAO
Emergency communication

Figure 1: Handling of a serious damage incident with BCM

Standard 200-4 also introduces a step-by-step model that makes it easier for less experienced users in particular to get started with BCM. Figure 2 shows the three stages of a BCMS: Reactive BCMS, Advanced BCMS and Standard BCMS:

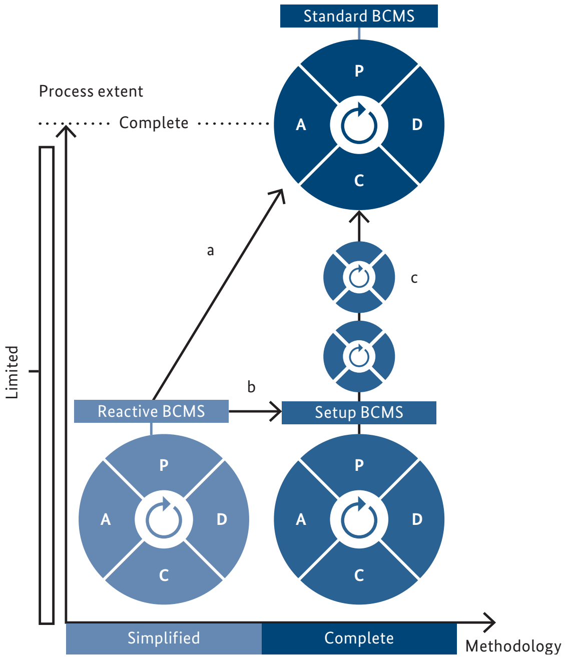


Figure 2: Overview of the stage model of BSI Standard 200-4

The respective stages differ in terms of the methodology to be applied and the scope of the process to be considered: The **Reactive BCMS** focuses on the fastest possible start that one must not dwell on due to a highly simplified methodology. It is a quickly feasible entry level that enables an institution without a previously implemented BCMS to carry out rudimentary emergency and crisis management.

The **Setup BCMS** allows for the step-by-step setup of a BCMS so that all business processes do not have to be considered in one big step. This ensures that important results can be achieved faster and the institution's own resources can be better allocated. The Setup BCMS first focuses on the most time-critical business processes in order to then successively increase the process scope until finally all business processes are examined in the Standard BCMS and all time-critical business processes are also appropriately secured.

The **Standard BCMS** represents a fully ISO 22301:2019 compatible BCMS. The BSI expressly recommends that a Standard BCMS be aimed at over the course of time, as this is the only way to ensure that all time-critical business processes are fully secured as necessary. ■

STAY IN CONTACT

The standard can be commented on during the Community Draft phase. You are welcome to send feedback to grundschutz@bsi.bund.de richten. Further information on all BSI activities related to BCM can be obtained from the BCM Info Group.

Further information on the BSI Standard 200-4 is available at:

https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html

Bridging the Gap between CC Certification and the BSI Approval Scheme

New Method Regulates how Products Certified by the BSI Can Be Successfully Approved

By Dr. Frank Sonnenberg, Section Classified Information Product Approvals

The BSI is mandated with ensuring the strengthening and maintenance of IT security in the classified information sector in accordance with Section 4 of Germany's Security Clearance Check Act (Sicherheitsüberprüfungsgesetz, SÜG), Sections 51 and 52 of the Classified Information Directive (Verschlusssachenanweisung, VSA) and Section 3 of the BSI Act. To this end, the BSI issues approvals for IT security products that are to be used for the protection of classified information on the basis of previously systematically conducted evaluations of those products. But in fulfilling this mandate, the BSI is faced with growing challenges.

IT security continues to develop with shorter technological innovation cycles in times of advancing digitalisation. At the same time, the current small market of approved products has to counter a constantly changing threat situation. This is no longer possible to an adequate extent, at least in parts. Not at last because of the growing product complexity, a timely, complete product evaluation and thus the provision of approved IT security solutions is not always possible.

In order to meet the described challenge, the approval process is constantly being further improved in order to identify any potential for optimization and to enable shorter reaction times to cover the consumer demand for IT products that are approved to handle classified information ("time-to-market").

In addition to the Qualified Approval Procedure, which has been successfully established since 2017, a bridge was built between the certification of products according to Common Criteria (CC) and the BSI approval scheme for the first time in 2019.

For this purpose, the BSI approval scheme was extended to include a supplementary sub-process – the so-called "Delta Evaluation." In this process, the evaluation results obtained in an earlier positive BSI certification are reused in the course of the evaluation activities necessary for approval.

This means that products that have already been certified can be transferred to the approval scheme, given that they are basically suited for the classified information market. This approach makes sense, since the efforts taken for a certification already represent a major part of the approval efforts and, due to the jointly used criteria and methods, their validity is basically comparable.

Likewise, the basic evaluation procedure and the evaluation philosophy of IT security products are very similar in terms of certification and approval. Any deviations do not really originate in the evaluation criteria themselves, but rather in the use, interpretation and recognition of the CC criteria and their methodology, which are aligned to the respective target audiences.

While certification generally bases its product evaluations on predefined so-called “assurance packages” according to the CC’s EAL table in order to gain comparability, the assurance aspects in an approval procedure are oriented towards the classification levels of the SÜG and the VSA.

The special challenge that this procedure has met for the first time is to harmonise the different paradigms of certification and approval. For this purpose, the normative description of the security functionality on the basis of “security functional requirements” as required in CC part 2 are transformed into the descriptive formulation of security requirements and functions as defined in Classified Information Requirements Profiles (VS-Anforderungsprofile) and “security targets” for approval. After this transition, the criteria defined for the integration procedure allow the re-use of the evaluation findings obtained in the certification for the approval in an efficient way.

Evaluation aspects that are not subject of CC certification but are essential for approval are additionally assesed by means of a delta evaluation within the scope of an approval procedure. As a general rule, the additional effort involved is significantly lower than for a conventional approval of non-certified products. The evaluation aspects based on the certification concern the evidence and evaluation with regard to the following approval criteria:

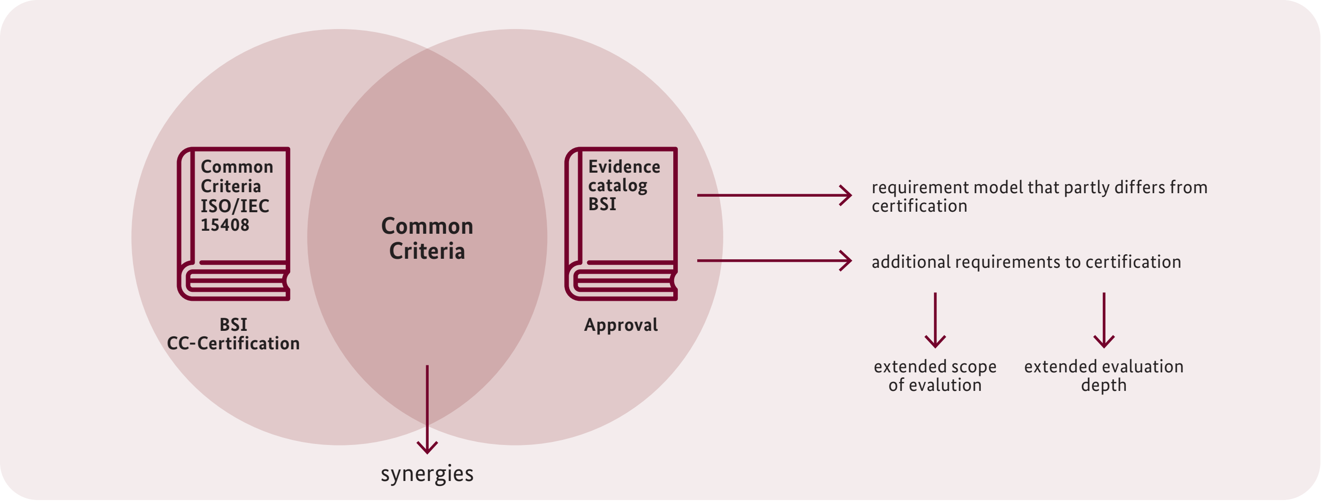
- Compliance with valid Classified Information Requirements Profiles (VS-Anforderungsprofile)
- Strength or effectiveness of the cryptography implemented
- Requirements for the underlying operational platform
- Emission security (CLASSIFIED INFORMATION CONFIDENTIAL and higher)
- Trustworthiness of product manufacturers

Such an integration procedure, like any approval procedure, can only be initiated if there is a need for the already certified IT security product to be used in the classified information sector as well. The conventional application and approval process for approval procedures documented in the approval scheme is then applied.

The advantages of using IT security products already certified by the BSI are quite obvious:

- The use of IT security products already known and evaluated in a BSI CC certification to meet the needs of the classified information product market
- An effective and timely expansion of the classified information product catalogue by taking into account an IT security market that was not originally in the focus of classified information.
- An efficient method of generating evaluation results for approval by utilising synergies from the certification and approval scheme.

By conducting initial validation procedures, it has already been proven that it is easily possible to transfer the evaluation results already achieved in the certification to the approval scheme, and thus an approval statement for the IT security product can be achieved by carrying out only a minimal delta evaluation. This means a significant reduction of the required evaluation effort and the duration of the procedure compared to the implementation of a complete approval procedure. ■


Common Criteria ISO/IEC 15408
BSI CC-Certification
Common Criteria
Evidence catalog BSI
Approval
synergies
requirement model that partly differs from certification
additional requirements to certification
extended scope of evalution
extended evaluation depth

Basic aspects of approval-specific requirements for the integration of CC-certified products into the approval scheme of the BSI

Secure and Modern Communication within the Federal Networks by using Wire

More than 30 Ministries and Agencies Use the Instant Messenger Wire for VS-NfD Classified Information (Restricted), and the Trend Is Rising

By Dr. Friederike Laus, Section Information Assurance Technology Evaluation, and Dr. Matthias Peter, Section Mobile Solutions for Classified II

Modern messengers have become an integral part of our everyday life. Since the end of February, the BSI has been evaluating Wire for use in federal agencies for VS-NfD classified information (Nur für den Dienstgebrauch - Restricted). While the use of Wire is initially limited to federal networks, in a further project phase, its use is to be extended to the public internet in order to enable modern communication between authorities and citizens.

VARIETY OF MESSENGER SOLUTIONS

Most recently, the COVID-19 pandemic convincingly demonstrated to most of us the wide variety of messengers and audio/video conferencing solutions. The choice, however, is drastically reduced if, in addition tu user-friendliness, aspects such as IT security and/or data protection also play a role and information is to be exchanged that is classified according to the VSA as VS-NfD classified information (Nur für den Dienstgebrauch - Restricted). Ultimately, none of the modern solutions for secure communication between participants within the networks of the Federal Government (NdB) and the public internet are left.

The last two aspects in particular led to the start of the project “Wire for VS-NfD” at the end of February. Since then, several BSI sections have been working intensively with the messenger Wire. In fact, the original initiative to launch the project came from the Federal Chancellery, which wanted to use the Wire messenger for modern VS-NfD communication in the context of the EU Council Presidency, which Germany holds in the second half of 2020.

MESSENGER WIRE AND THE DOUBLE RATCHET PROTOCOL

Wire is an instant messenger that can be used on smartphones and tablets as well as on Windows, macOS and Linux computers. Within the scope of the evaluation, the enterprise version of the Wire app was considered, which, however,does not differ from the standard version in the essential cryptographic components. The main functionality of the Wire app is the exchange of messages, pictures or other files between two users, whereby group chats are also possible. Figure 1 shows an example of a chat history. All messages between the chat participants are end-to-end encrypted and synchronised on up to eight user clients. The communication between the app and the backend server in the NdB is additionally TLS-encrypted. The Double Ratchet Protocol [1] known from the messenger Signal is used for message encryption. With slight modifications, this protocol is also part of other messengers and is nowadays used by more than one billion people worldwide. The protocol essentially consists of three phases: an initial key exchange (X3DH, "Extended Triple Diffie-Hellman") to generate a common secret, and an asymmetric and symmetric "ratchet," which also give the protocol its name. One of the basic ideas of the protocol is to exchange new keys with every message. The figurative ratchet of the key material is thus quasi moved and locked such that it is not possible for an attacker to return from a later to an earlier stage of the protocol and decrypt previous messages. A simplified representation of the asymmetric ratchet is shown in figure 2. The security of the protocol, which is currently regarded as state-of-the-art in the field of instant messaging, has been analysed in a number of research projects (e. g. [2], [3]). Furthermore, Wire allows to conduct end-to-end encrypted (group) telephone calls and, on a small scale, video conferences. Here, the WebRTC protocol is used.

CROSS-SECTIONAL COOPERATION

The Wire app was tested intensively not only theoretically but also practically. Thus, a preliminary VS-NfD approval for the on-premise use of Wire in the Federal Administration was issued in time for the start of the EU Council Presidency in early June. This initially covered the use of the app on desktop PCs as well as SecuSUITE for Samsung Knox devices (Android) and was extended at the beginning of October to include SecurePIM Government SDS (iOS system solution). The messenger met with a pleasingly positive response and was already in use in many places after only a short time. It is currently being used by a total of around 2,000 users in 30 ministries and public agencies (as of September 2020), including the BSI.

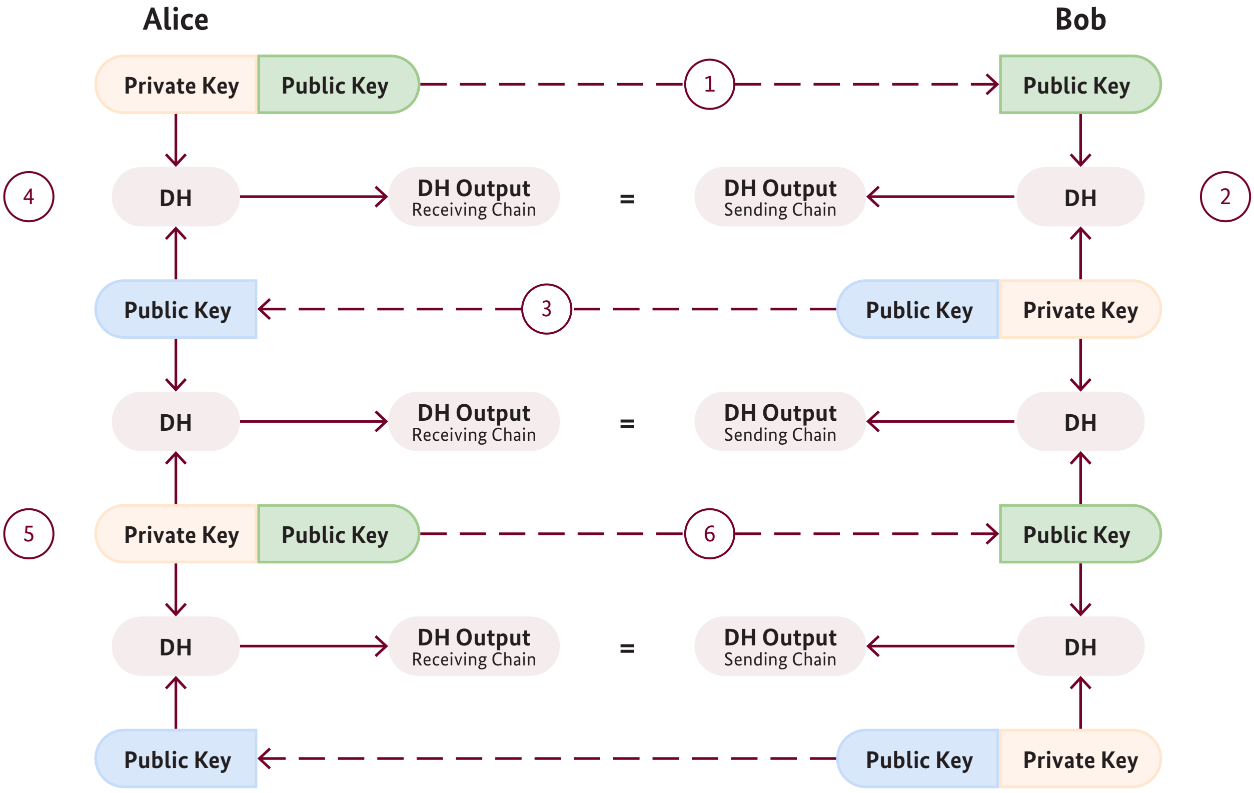


Figure 1: Simplified representation of a section of the asymmetrical (Diffie-Hellman) ratchet. The common Diffie-Hellman secrets are used to calculate keys for encrypting and decrypting messages using the symmetric (Sending and Receiving) ratchets. Alice's sending ratchet corresponds to Bob's receiving ratchet and vice versa.

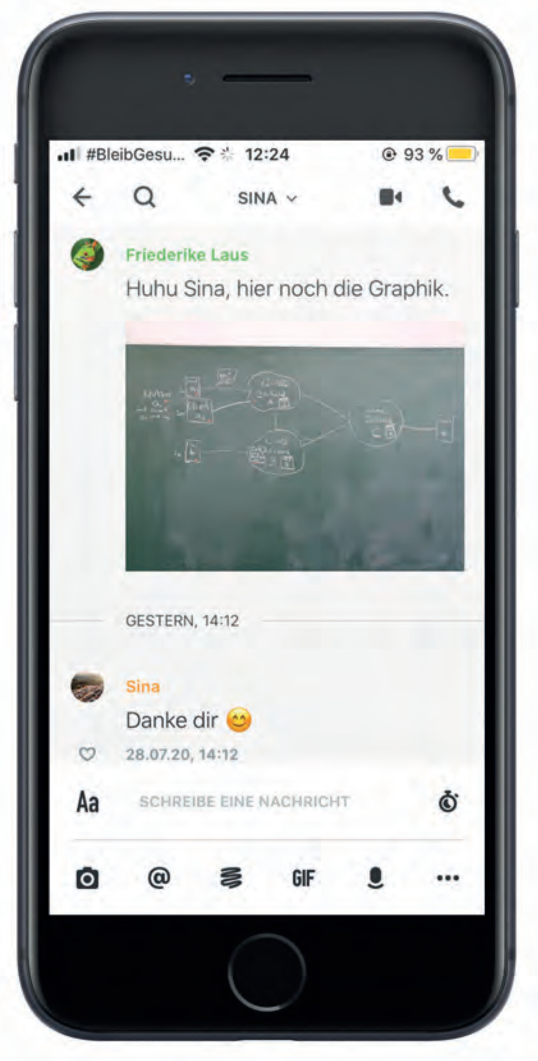
1.) Alice sends a message to Bob together with her public key.
2.) Bob calculates a common Diffie- Hellman secret with Alice's public key and his private key.
3.) Bob sends his public key to Alice together with his next message.
4.) Alice calculates the common Diffie-Hellman secret with Bob's public key and her private key.
5.) Alice generates a new key pair.
6.) Alice sends a message to Bob together with her new public key.

The project is also a good example of successful cooperation between different sections of the BSI. Whether it is Section KM 12 for approval issues, Section KM 15 for aspects of VS-IT, Section KM 22 for cryptographic issues, Section KM 23 (iOS) and KM 24 (Android) that focus on mobile solutions, Section KM 13 for EU/NATO issues or Section BL 33 and BL 34 for network connections – many colleagues were and are involved in the project and are strongly committed to it. In fact, the tight schedule would not have been adhered to if each and every one of them had not taken on tasks and provided support across section boundaries.

FURTHER PROJECT DEVELOPMENT

The Wire project is far from being completed with the issuing of the preliminary approval for VS-NfD, however. At present, a further development of the product as well as significantly more in-depth evaluation are pending, the goal of which is a VS-NfD approval, which was not possible due to time constraints. In this context, for example, the Double Ratchet protocol is to be replaced by the so-called MLS Standard (Messaging Layer Security). One of the main concerns in the development of MLS was to standardise different messaging protocols to such an extent that different applications can reuse the source code and, in particular, uniform security analyses are easier to carry out. Alongside the company Wire, a number of well-known firms (including Mozilla, Twitter, Cisco, Google, Facebook) as well as research institutes (INRIA) and universities (MIT, University of Oxford) are involved in the development of the standard.

The federation with the public internet, so that communication is possible not only within the networks of the authorities but also across networks, will be yet another milestone in the project. Although there are still a number of challenges to be overcome by then, it is hoped that a modern product will be available at the end of the road that will enable modern and at the same time secure communication between authorities and citizens. ■



Friederike Laus

Huhu Sina, hier noch die Graphik.

GESTERN, 14:12

Sina

Danke dir 😊

28.07.20, 14:12

SCHREIBE EINE NACHRICHT

Figure 2: Example of a chat history in Wire

More information:

https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

https://eprint.iacr.org/2018/1037.pdf

https://eprint.iacr.org/2016/1013.pdf

https://datatracker.ietf.org/wg/mls/about/

THE BSI IN HEALTHCARE

Special Feature: Cyber Security in Healthcare

Foreword by Bernd Kowalski, Head of Cyber Security in Digitalization and Electronic Identities

An IT security incident occurred on 10 September 2020 at the University Hospital of Düsseldorf. A cyber-attack crippled the hospital's emergency care, which was then disconnected from acute care for 13 days. The BSI immediately set up continuous contact between the hospital and the Cyber Response Centre and supported the people in charge at the hospital on site by providing a mobile task force.

The incident once again demonstrated the huge importance of designing cyber security in the healthcare field. Not only do IT security incidents in this area of critical infrastructures threaten life and limb in case of emergency, all players in the healthcare system – from patients to hospitals and health insurance companies – benefit from securely designed digitalisation. Digital healthcare can make people's lives easier, reduce long distances and waiting times and provide rapid support in the event of illness or emergency. That is why the digitalisation of the healthcare system is a key issue for the future. Nevertheless, all of the benefits of eHealth would be inconceivable without information security.

In this issue of the BSI Magazine, we would like to present some of the application areas that are currently the focus of our work on digitalisation in the healthcare field: the corona warning app, the further development of the electronic health care card, emergency data management and the electronic medication plan in connection with drug therapy security, the electronic patient file, the telematics infrastructure and the IT security of medical devices with the ManiMed project – manipulation of medical devices.

The BSI provides support in all of these fields with specifications, technical guidelines and assistance for authorities and companies in order to find practicable and secure solutions very quickly. Close cooperation with partners such as gematik, the Federal Ministry of Health (BMG), the Federal Commissioner for Data Protection and Freedom of Information and the Federal Institute for Drugs and Medical Devices is a matter of course. The goal is to ensure that the opportunities offered by digitalisation can be used securely, especially in healthcare.

Transparent, Secure, Useful

Digital Health Applications

By Tim Griese, Staff Strategic Communications and Press, Dr. Dina Truxius, Alexandra Mayer, Emanuel Müller and Christian Kleinmanns, Section Cyber Security in Healthcare and Finance.

The healthcare sector is a focal point of digitalisation in Germany. The electronic patient file, the measurement, storage and evaluation of health data via app and the video consultation hour – these are just a few examples of digital technologies that are currently transforming the German healthcare industry. The Corona Warning App, which has already been downloaded 17 million times, also belongs in this category of applications. The BSI has been on hand to advise the developers from the very beginning to ensure the highest level of IT security every step of the way.

According to Section 33a of the German Social Security Code, Book Five (SGB V), people with statutory health insurance are entitled to receive so-called digital health applications under certain conditions. These “apps on prescription” facilitate communication between the various players in the healthcare system and enable individual patients to better manage their own health, through apps that measure the pulse rate or sleep rhythm, analyse symptoms or establish contact with doctors, for example.

Digital health applications connect the user with the appropriate services and act as communication nodes. Their basis is the insured person’s medical data, which can be exchanged between doctors and patients, but also between individual health care providers, using modern information and communication technologies.

The health applications process sensitive and particularly personal data that needs to be protected. If an attacker can manipulate a third party’s health data and thus violate its integrity, this could have a significant impact on therapy decisions and ultimately concern patient’s health.

The BSI therefore developed a Technical Guideline (TR) back in 2019, independently of COVID-19, and published it in April 2020, which, when applied, makes it more difficult for unauthorised persons to access this data. The TR “Security Requirements for Digital Health Applications” (BSI TR-03161) can basically be used for all mobile applications that process and store sensitive data.

The TR can be used by developers of mobile applications in the healthcare section as a guide for creating secure mobile applications. It is aimed at manufacturers of digital health applications for mobile devices. It defines the state of the art and can be used in the future, as part of a manufacturer’s declaration or as a basis for certification, for example.

THE CORONA WARNING APP

The Corona Warning App (CWA), which has been available for free download in Apple and Google App Stores since 16 June 2020, is also basically a mobile health application. Its great success – by the end of August 2020, more than 17 million users had downloaded the app – sets international standards, as even Great Britain’s Prime Minister Boris Johnson had to acknowledge. When he told the opposition in the British House of Commons on 24 June 2020 that no country in the world had a functioning contact-tracing app, he was corrected by opposition leader Keir Starmer: “But Germany does.”

After a European solution that was initially planned to offer centralised data storage was rejected by the German government, Deutsche Telekom and SAP were commissioned to develop an app with decentralised data storage and bring it to market maturity. The app had to be compatible with other European solutions. After its completion, the Corona Warning App was published by the Robert Koch Institute (RKI).

The Corona Warning App uses Bluetooth to measure the distance and duration of encounters between people who have installed the app. The smartphones “remember” encounters when the criteria for distance and time set by the Robert Koch Institute (RKI) are met. The devices then exchange random codes with each other. If people who use this app are tested positive for COVID-19, they can use the app to voluntarily inform other users.

The BSI has provided consulting services from the very beginning of the development of the Corona Warning App and the associated comprehensive security concept to ensure the highest level of IT security every step of the way. A task force was set up at short notice and worked in interdisciplinary cooperation with the app developers at SAP and Telekom as well as with the Fraunhofer-Gesellschaft, the Helmholtz Centre for IT Security CISPA and the Federal Commissioner for Data Protection and Freedom of Information (BfDI). For example, the BSI supported the open source development process by conducting code reviews and penetration tests of the code provided for the front-end and back-end. All vulnerabilities found were and still are being made transparent and eliminated in close cooperation with the Federal Government, the Robert Koch Institute and the developers of the app. Critical and serious vulnerabilities were fixed already before the app was launched.

In order to create the transparency necessary for broad acceptance, the app’s concept and programme code (source code), as well as the underlying server architecture and other documents about the app’s functions, were published on the development platform GitHub (open source). Interested parties were thus able to follow the development and programming of the app and participate in its design.

The experts at the BSI were also significantly involved in the development and implementation of the security concept. The Corona Warning App is easy to use, technically up to date and does not pose any data protection concerns. It also shows that IT security is not an obstacle to digitalization projects. On the contrary: with high security standards, many users can be reached and, just as importantly, acceptance can be significantly increased. According to a study conducted by Oxford University, a tracing app starts to take effect as soon as 15 percent of the population participates (https://jme.bmj.com/content/46/7/427).

The CWA reached this value after only a few weeks. The BSI will closely accompany the further development of the Corona Warning App with regard to its IT security features in productive use as well.

DESIGNING DIGITAL HEALTHCARE TO BE SECURE

The BSI is constantly looking into the fields of application in which risks could arise from digitalisation and how these risks can be made calculable and controllable. One example is the further development of the electronic health card (eGK). Here, the focus is currently on the development and use of new applications such as emergency data management (NFDM) and the electronic medication plan (eMP) in connection with medication therapy safety (AMTS) and the electronic patient file (ePA) (see also the article "Strong Upswing for Digitalisation in Healthcare" on page 20).

The BSI has also drawn up corresponding Technical Guidelines (TR 03154, TR 03155, TR 03157). They define the state-of-the-art and serve to check whether the connectors used in medical practices and hospitals, among other places, meet the gematik requirements approved by the BSI.

In the future, data for medical emergencies and electronic medication plans can be securely stored on the eGK and be retrieved in case of an emergency. In the case of the electronic medication plan, the attending physician can compare new medications to be prescribed with current medications, thereby minimising potential risks.

In a further step, an electronic patient file (ePA) will be available to those with statutory health insurance in addition to the existing functions, which they can use voluntarily. In accordance with the German Appointment Service and Care Act (Terminservice- und Versorgungsgesetz, TSVG) passed by the German Parliament on 14 March 2019, all statutory health insurance companies are obliged to offer their insured persons such electronic patient files by 2021 at the latest. Physicians and hospitals may then, with the consent and approval of the insured person, securely access the respective file in order to enter or view the corresponding medical data of the patient.

Even medical treatments that span multiple practices can thus be coordinated, and multiple examinations that may be stressful for the patient can be avoided. The access by the insured to their individual files is to be made possible by means of their own devices (PC, smartphone or tablet) and software. In addition, it should also be possible to access their own ePA with a secure device in the public offices of the respective health insurance companies.

The IT security of medical devices is yet another focus of the BSI's work in the area of healthcare. The ManiMed project – Manipulation of Medical Devices (see article on page 18) – started in early 2019 and is intended to provide as realistic a picture as possible of the Cyber Security situation of networked medical devices in the following categories: Implantable pacemakers and accessories, insulin pumps, ventilators, patient monitors and infusion pumps. The results of the security-related investigations will be published at the end of 2020. In the long term, they are to be incorporated into standardisation and norms where they will help the BSI to draw up Technical Guidelines.

BLUEPRINT CORONA WARNING APP

Like the Corona Warning App, many other digitalisation projects of the Federal Government (not only) in the healthcare field live from citizens' trust. This trust is created through transparency and the best possible IT security. The BSI plays a creative role in the Federal Government's key digitalisation projects, making its expertise available and ensuring the highest level of IT security.

Digitalisation and networking in healthcare is bringing progress because patients can be cared for more comprehensively, and the costs are falling. But they also involve risks if IT security is not thought through and implemented from the very first step. This is precisely what the BSI does thanks to its professional expertise that has grown over decades, its networking with all players and its commitment. ■

Wanted:

Digital Talents

(f/m/div.)

For our Locations in Bonn and Freital

Scan and apply!

bsi.bund.de/jobs

Federal Office
for Information Security

Are you enthusiastic about diverse, varied and challenging tasks? Do you enjoy working on topics related to advancing IT security inside a team? We are looking for talented people, whose heart beats on the digital side and who want to help ensure that people can trust the digital world and that digitalisation becomes a success story.

What we wish for: A degree in computer science, economics, business administration, administrative informatics, IT security or IT management and commitment to exciting topics in the field of Cyber Security.

Visit our career page at **www.bsi.bund.de/karriere.**

For further information: **bewerbung@bsi.bund.de** or call us at +49 228 99 9582 6388.

IT Security and Vulnerabilities in Medical Devices

Results of the BSI Projects eCare and ManiMed

By Dr. Dina Truxius, Section Cyber Security in the Public Health and Financial Services Sectors

Hacked medical devices – a disconcerting idea and topic that concerns and can affect not only patients and doctors but also people worldwide. The project work of the BSI casts light on the IT security of certain medical devices.

ECARE – DIGITALISATION IN GERIATRIC CARE

With the advance of digitalisation and networking in healthcare, more and more intelligent systems are being developed and manufactured for the sick and elderly. All of these products are designed to offer comfort and relief for nursing staff and ideally enable patients to live more self-determined and comfortable lives. In the course of the project, a market survey of products that have been offered in this market over the last two years was first carried out. After completion of the market survey, six products from various categories, such as reminder services or devices for measuring vital data, were selected for pentesting (low depth of testing).

MANIMED – MANIPULATION OF MEDICAL DEVICES

In most cases, the security of medical devices is more closely related to patient safety than to their IT security. The trend towards networking is increasingly affecting medical devices as well, however. Likewise, European and national legislation is focusing on this topic. In the ManiMed project, two networked medical devices from each of the following five different device classes were examined in terms of IT security (high penetration depth), since not the complete portfolio of all medical devices available on the market could be tested as part of the project:

- Implantable pacemakers or defibrillators and their accessories
- Insulin pumps
- Ventilators
- Patient monitors
- Infusion pumps

Further conditions of the market survey were that all devices have as many interfaces as possible and not be on the market in Germany for more than five years. Following the market research, the products were procured accordingly or made available by the manufacturers and tested within the framework of the project. The manufacturers were informed of the vulnerabilities found and the countermeasures taken and a coordinated process was carried out jointly (Link to article on Coordinated IT Security).

CONCLUSION

Weaknesses of different criticality were found for all devices in both projects. In nearly all cases, IT security and not patient safety was affected. For example, the more critical weaknesses included the disclosure of sensitive device data or credentials. The vast majority of manufacturers reacted accordingly by assessing the risk, providing updates and improving the current products and their successors in terms of their IT security features.

Both projects showed that the transparent and open handling of vulnerabilities and the appropriate exchange of communication are necessary in order to build, maintain and strengthen trust in the long term. Ideally, the results of both projects are already being incorporated into standardisation or standardised procedures and support the BSI in preparing technical guidelines and recommendations. The BSI also sees a great need for the joint work to be continued after the project work is completed in order to improve Cyber Security. There have been no projects of this kind at either the national or international level to date. Therefore, the results are ground breaking for the approach in the area of networked healthcare and medical products. ■

Strong Upswing for Digitalisation in Healthcare

Current Developments in the Telematics Infrastructure and Outlook

By Alexandra Mayer, Section Cyber Security in the Public Health and Financial Services Sectors

Digitalisation in the field of healthcare has received a strong boost in recent years. The telematics infrastructure (TI) has been developed to network various players in this sector. The core of this TI is the connector. This ensures a secure connection and thus enables networking within the healthcare system. The connector is the connection to the TI for every doctor's practice, pharmacy, hospital and other medical facilities.

Insured person standing data management (Versichertenstammdatenmanagement, VSDM) is one of the first applications of TI. Insured person master data, which includes personal data and health insurance details and is stored on the electronic health card (eGK) of those with statutory health insurance, is compared with the data of the health insurance company and updated. The secure connection of TI is used for this purpose.

CURRENT DEVELOPMENTS OF THE TI

Software updates for connectors were provided during the summer of 2020 to activate other TI services:

Emergency data management (Notfalldatenmanagement, NFDM) enables every insured person to store medical information relevant to emergencies on his or her eGK, which can be of great relevance to the attending physician in an emergency. In addition to pre-existing conditions, allergies and medications, it is also possible to deposit a "personal declaration" here that provides information on whether medical powers of attorney, an organ donor card or patient declarations are available, for example, and where these can be found. In an emergency situation, this information can make a decisive difference for the treatment and thus the insured person.

Besides emergency data management, the electronic medication plan (eMP) is activated and stored on the eGK. The eMP contains all prescription medicines that a patient is taking, as well as self-medication. The treatment of the insured person is to be made easier and better, as different doctors treating the patient can better coordinate their medications and thus avoid interactions.

Besides these two services, communication between different physicians, hospitals, pharmacies, associations of statutory health insurance physicians, health insurance companies and other institutions will be simplified through communication in medicine (Kommunikation im Medizinwesen, KIM). With the help of KIM, all electronic communication can be sent as secure e-mails. These can be doctors' letters and findings as well as certificates of incapacity to work. The authenticity of the documents is guaranteed by a qualified electronic signature (QES), which is equivalent to a signature. KIM will be further developed over time, for example, the sending of a certificate of incapacity to work to health insurance companies is planned for early 2021.

THE NEAR FUTURE OF THE TI

The electronic health record (elektronische Patientenakte,

ePA) will be introduced from 1 January 2021. In the long term, the ePA is expected to replace the traditional paper-based patient record. The insured person will then not only have unrestricted access to his or her ePA and thus to all his or her medical data, but will also be free to decide which documents can be viewed and changed by whom. Log data can also be viewed, making it possible to track who changed which data and when. In addition to current findings and treatments of the insured person, it will also be possible to store documents such as the vaccination card.

The insured person will be able to access his or her own ePa via a mobile application (app) utilising a personal mobile device. In this way, the patient data can be viewed at any time while on the move. At the same time, the informational self-determination of the insured person is ensured.

THE DISTANT FUTURE OF THE TI

From 1 July 2021 on, the electronic prescription (E-Rezept) will be available. Recipes will be issued digitally from this date. Insured persons will be able to manage prescriptions via an app on their own smartphones. A prescription can either be sent directly to the desired pharmacy or a corresponding token can be presented and scanned at the pharmacy. Of course, the app is not mandatory, the token can be printed out by the prescribing doctor, so that a different type of paper-based prescription is available.

IT SECURITY OF APPLICATIONS

The NFDM, eMP, ePA and E-Rezept applications will all be introduced on a voluntary basis. Medical data is highly sensitive data and has a high need for protection. In order to meet this need for protection, the BMG, gematik, BfDI and BSI are working together on the project. The security of the various applications is always the focus of development, is constantly being further developed and kept at the current state of the art. ■

Security Gap Discovered in a Medical Device – What Now?

The Coordinated Vulnerability Disclosure Process Helps to Manage Vulnerabilities

By Dr. Dina Truxius, Section Cyber Security in the Public Health and Financial Services Sectors

Vulnerabilities in IT systems can exist at any time. Even medical devices are no exception. It is therefore important to proceed in a coordinated manner and to follow a corresponding process if vulnerabilities are discovered in (medical) devices.

The maturity of a company with regard to IT security is measured not only by the way in which vulnerability reports and IT security issues are handled, but also by how the relevant information is communicated and the resulting actions are coordinated. Companies that have experience in this area inform their customers and publish vulnerabilities as soon as they have been eliminated. This is done on an international level in the form of information to the relevant users, through ICS advisories prepared and published by CISA (Cybersecurity and Infrastructure Security Agency) in the US and through the registration of CVE (Common Vulnerabilities and Exposures). The BSI supports this transparency, uses and integrates internationally established processes and is therefore in close contact with the American authorities in order to contribute cooperatively to more closely coordinated IT security.

THE "RIGHT" WAY TO DEAL WITH VULNERABILITIES

An ideal process with regard to the handling and subsequent publication of security vulnerabilities is characterised by a high degree of equal treatment, communication and cooperation between all parties involved, regardless of whether it is a networked medical device or a smart washing machine. The parties involved are often security researchers who discover a vulnerability and the manufacturers of the respective product. Depending on the product category and area of responsibility, the competent authority or a CERT (Computer Emergency Response Team) may also be involved.

It is desirable that a so-called Coordinated Vulnerability Disclosure Process (CVD) is carried out by all parties involved after receiving information on vulnerabilities in a product. This process is based on a trustful exchange and continuous cooperation. During the entire term of the CVD, no other party, except the parties involved, receives knowledge of the vulnerabilities found. After completion of the CVD, transparent and open communication concerning the vulnerabilities should take place (advisories, etc.) in order to maintain IT security at a high level and to inform other manufacturers of any possible vulnerabilities.

CVD PROCESS BASED ON THE EXAMPLE OF THE MANIMED PROJECT – MANIPULATION OF MEDICAL DEVICES

The procedure in the ManiMed project (see article on page 18) emphasises the equal treatment of manufacturers and is therefore based on a CVD in which the IT security gaps found are not published for the time being (at least 90 days). This gives the manufacturer time to eliminate the vulnerabilities and to develop, check and roll out the corresponding security updates.

All products are subjected to in-depth IT security tests during the project. The weak points found are communicated to the manufacturer in the form of a detailed test report, technically described and explained in detail. Mitigation measures are proposed already in the test report, and the individual vulnerabilities are classified and quantified according to CVSS V3 (Common Vulnerability Scoring System). This system allows for a subdivision of vulnerabilities into INFO, LOW, MEDIUM, HIGH and CRITICAL, whereby critical vulnerabilities are to be eliminated immediately. All vulnerabilities that fall under the MEDIUM category should be fixed with the next update. If critical vulnerabilities are found which the manufacturer cannot or does not wish to remedy, the BSI may, based on its statutory duty under Section 7a BSIG, request the manufacturer to submit a statement and, if necessary, issue a warning under Section 7 BSIG.

The manufacturer then works out a (residual) risk assessment with regard to safety and security (patient safety and IT security) from the test report made available as well as a schedule and, if necessary, initiates internal processes. If the manufacturer can identify patient risk in the course of his risk assessment on the basis of the vulnerabilities found, the Federal Institute for Drugs and Medical Devices (BfArM) is involved in the process as the competent authority. The vulnerabilities should only be published in consultation with the manufacturer and, if necessary, be presented at relevant IT security conferences once they have been remedied. After the project has been concluded, the manufacturer is not permitted to promote his tested product as either BSI-certified or BSI-tested, as neither the depth nor the scope of testing corresponds to certification. It must always be remembered that even a "freshly" tested product might again exhibit possible weaknesses. IT security is a continuous process that should be considered during the entire product lifecycle. ■

THE BSI

New IT Study Programme "DACS" at the Federal University of Applied Sciences

By Alessandra Krüger, Section Human Resources Development

Various Cyber Security incidents in recent years, a new quality of cyber-attacks and the growing digitalisation of the state, economy and society show that IT and Cyber Security aspects are becoming increasingly important in public administration. The training of qualified young people on IT security in the Federal Administration makes a valuable contribution in this respect. The new study programme "Digital Administration and Cyber Security" (DACS) was therefore launched at the Federal University of Applied Sciences in Brühl in October 2020. The BSI and other authorities are participating in the selection process with approximately 10 study places per year and by offering internships. The goal is to be able to offer the students permanent positions afterwards. Of course, the BSI's students focus more on "Cyber Security" than on "digital administration."

WIDE VARIETY OF CONTENTS

In addition to the basics of IT security, forensics and cryptography, knowledge of IT project management and public law will be taught – a perfect alignment with the needs of the authorities and thus also with those of the BSI. Two six-month internships at local authorities will provide for a deepening of the knowledge acquired during the course of studies and support the students' decision-making process for a later subject area. The professors are experienced in administration and are familiar with the current needs and standards of the federal authorities, which they convey to students in a practical manner.

STUDYING IN A DUAL SYSTEM AND EARNING OWN MONEY

From the beginning of their studies, the students hold temporary civil servant positions that come with a salary that will be just over EUR 1,500 gross in 2020. In contrast to lecture halls that have to be shared with hundreds of other students, the course size is 25 students. Students can choose from a wide range of sports activities directly on campus and dormitories are available directly at the university depending on availability. The lecture times from 8:00 a.m. to 3:30 p.m. are family-friendly. The course of study ends with a diploma in public administration and is practically linked to a job guarantee from the respective internship authority.

Applications can be sent via the university's website. Further information and the link to the announcement can be found at https://www.bsi.bund.de/karriere. ■

f.l.t.r:
Thomas Seider, Dennis Brykin, Lukas Altmeier, Leonard Keding, Gianluca Carcereri de Prati und Kay Kretschmar

Strengthening the Cyber Defence Force: New BSI Office in Freital

The Federal Minister of the Interior, Building and Community Horst Seehofer and the Minister of the Interior in Saxony Prof. Roland Wöller officially opened the second office of the BSI in Freital/Saxony in July 2019.

By Joachim Weber, Setup Staff Unit Saxony

The BSI is a supporting pillar of Germany's security architecture and thus the central contact for all matters related to Cyber Security. The digitalisation of Germany would be inconceivable without adequate consideration of Cyber Security, therefore an appropriate involvement of the BSI in this important project is indispensable. The new office of the BSI in Freital with its 200 workplaces is of great importance in this context. The current shape of digitalisation is characterised by new areas of technology such as the 5G infrastructures currently under construction or digital consumer protection. The main tasks of the BSI employees in Freital will be to take the Cyber Security issues arising in this context into account and develop practical solutions for the benefit of the state, the business world and society as a whole. They will work very closely with their colleagues at the BSI in Bonn and Saarbrücken.

NUMEROUS TECHNICAL AND PROCEDURAL INTERFACES WITH ALL OF THE BSI'S DEPARTMENTS

The BSI underwent a major reorganisation in 2019/20, which officially came into force on 1 August 2020. The characteristic feature of this reorganisation is the creation of an integrated BSI value chain, which establishes the BSI competence and service areas in a process-oriented and cross-departmental manner. The organisational units set up at the site in Freital are characterised by a large number of technical and procedural interfaces with all departments of the BSI. While the office in Freital is being set up, these internal interfaces will be supplemented by appropriate contacts in the areas of administration, the business world and society.

The organisation of the site in Freital is based to a large extent on the establishment of the two specialist branches SZ 3 and WG 3, which represent the thematic complexes "Cyber Security in Mobile Infrastructures and Chip Technology" and "Digital Consumer Protection, Cyber Security for Society and Citizens." On the one hand, the thematic priorities are the elaboration of technical foundations and security requirements with a view to the new 5G infrastructure and the implementation of regular audits to ensure compliance with the relevant BSI specifications. In this context, the BSI will certify relevant network components, for example, and ensure the provision of chip-based eID technologies for mobile applications and award a corresponding IT security label. On the other hand, digital consumer protection, as far as questions of Cyber Security are concerned, will be sustainably realised by establishing two specialised sections with additional organisational units for market monitoring, a consulting service and a service centre for Cyber Security information. In addition to these two specialised branches that will be represented in Freital by a total of ten sections, there are also many other BSI specialised sections that cooperate closely with their departments in Bonn and will serve regional needs in Freital.

PERSONNEL RECRUITMENT AND SEARCH FOR NEW PROPERTY IN FULL SWING

The recruitment of staff for the office in Freital is currently in full swing. The first new colleagues have already been recruited and are being intensively trained on what are usually new tasks for the BSI headquarters in Bonn by their "more experienced" counterparts. The individual employee-related training concepts created facilitate the familiarisation phase, which will be completed after around six months and then lead to employment in Freital. Since not all of the employees of the BSI in Freital can be hired at once, many of the newly recruited employees are being trained in Bonn for a longer period of time. This is an exciting and challenging task for all those involved.

The provision of a property for the new branch office in Freital in line with time and demand is also proving to be an exciting challenge, as the constantly growing number of employees resulting from hiring has to be synchronised in terms of time and space requirements. For this purpose, the BSI is working intensively with those locally responsible and the very helpful offices of the city of Freital and the BImA (Bundesanstalt für Immobilienaufgaben – Institute for Federal Real Estate).

The opening of the second BSI office in Freital offers an excellent opportunity for the Federal Government as well as for the region of Saxony, to concentrate the cyber defence force locally and to design, bundle and sustainably further develop forward-looking security topics with important impulses from authorities, companies and the science community in close cooperation with all parties responsible. ■

“Free State of Saxony Wants to Play Leading Role in Cyber Security”

Interview with State Secretary Thomas Popp, who is also Commissioner for Information Technology (CIO) of the Free State of Saxony.

■ **Dear Mr. Popp, You have taken on many different administrative tasks in Saxony to this date. What have you gained for yourself from this wealth of experience and your work as CIO of the Free State?**

At the various stages of my professional career, I have always had to deal with digitalisation. In particular in tax administration, which is considered to be the forerunner of the digital revolution in administration, I was able to play a key role in the modernisation and digitalisation of administrative processes. In the process, I learned a lot about change processes in general and how people need to be supported with this change, in addition to my specialist knowledge. Of course, these experiences also help me as State Secretary for Digital Administration and the Modernisation of the Public Administration with the task ahead of us of shaping the administration of the future in a more modern and digital way. In my more than twenty years of work for the Free State, I have met many interesting people who have given me useful impulses for my work and often opened up new perspectives for me. Precisely because the upcoming digital transformation affects all areas and thus brings about fundamental changes for everyone, it is important to listen on the one hand and to exchange ideas on the other.

■ **As a Federal Office in Bonn, we have now also taken root in Saxony. What was the reason for you to say that we offer the BSI a second home in the Free State?**

The Free State of Saxony wants to play a leading role in the area of Cyber Security and show in cooperation with the Federal and State Governments as well as science and industry that a bundled defence in the cyber space is more effective because cyber threats do not stop at state borders. The state capital and the business and innovation location Dresden, with its proximity to the Czech Republic and Poland, is a particular example of this. As the largest location for the semiconductor industry in Europe, Dresden offers important points of contact for Cyber Security. Leipzig is the booming region in Germany and is consolidating its reputation as a technology location. But also beyond these two metropolitan regions, Saxony holds great potential when it comes to well-trained specialists thanks to its university landscape, especially with regard to the special qualifications in Cyber Security. So, it is only logical for the BSI to have a strong base in this region and to strengthen cooperation on a personal level as well.

■ **With Komm24 GmbH, you have founded your own municipal IT company for the Free State of Saxony. The Saxon administrative network was recently certified by the BSI – two important milestones in terms of digitalisation and IT security. How does this help the municipalities, the economy and the people on site? What is the State government doing for information security in Saxony?**

Information security is one of the cornerstones on which digital management is built. Without a comprehensive guarantee of information security, we will not succeed with the digital transformation process. For example, citizens and companies will only use these services if we create simple digital access to administrative services and at the same time guarantee comprehensive information security.

In concrete terms, this means that every digital administration offer takes information security aspects into account as early as the conceptualisation phase and these are then applied in development and technical implementation. Furthermore, administrative staff and users of the procedures must be sensitized to information security risks, and this must be done on an ongoing basis. I am committed to these aspects in the current legislative period.

■ The BSI will primarily develop the security of future technologies in Freital. But digital consumer protection as a new BSI task will also be driven forward from Saxony. Where do you see possible joint fields of action and projects of the BSI and institutions in Saxony?

I am pleased that with the BSI there is a competent player for digital consumer protection at the federal level. A survey on Cyber Security commissioned by us in 2018 shows how necessary this is: Citizens want more information and more help offers. But they don't know who they can ask about this. I hope that the BSI can fill this gap. As the Free State of Saxony, we would like to provide them with assistance. Before the restrictions imposed in response to the COVID-19 pandemic, we were very active in Saxony by holding awareness events on Cyber Security for citizens under the motto "The hackers are coming." Last year alone, we organized 22 events with over 2,200 participants. The focus was also on the European Cyber Security Month, which is coordinated by the BSI in Germany and in which we were involved from the very beginning.

■ There is one topic you simply cannot avoid in 2020: Corona. In an interview, you spoke of a new drive in the area of IT security in the wake of the pandemic. What do you mean by this and how have you as the Free State of Saxony mastered this difficult time?

Like all administrations, I think we were faced with the challenge of remaining capable of working. Corona forced us into a kind of digital collaboration that seemed unthinkable only weeks before. From one day to the next, videoconferencing and other collaboration platforms were set up and things were made possible that had previously been debated at length. The Saxon state administration also remained capable of working in difficult times because, on the one hand, we had done good preparatory work and, on the other, because we had a strong state-owned IT service provider and a functioning information security organisation that helped with taking pragmatic approaches. However, we are still aware that if we want to continue with digitalisation at this rapid pace, we need to bring the security experts into the team. They are the guarantors that administration is not only modern and digital, but also meets high security standards. ■

Brief Profile Thomas Popp

Thomas Popp was born in Schweinfurt on 8 November 1961. The fully qualified lawyer began his career in the civil service in 1992 as a lecturer at the Civil Service College in Herrsching. Between 1998 and 2004, Thomas Popp was responsible for the development of the performance comparison between tax offices in the tax administration as project coordinator for the Free State, was the head of various departments of the Freital Tax Office and took over the position of Head of the Freiberg Tax Office in 2004.

He moved to the Saxon State Ministry of Finance in 2005. In 2010, Thomas Popp was entrusted with the management of the Upper Finance Directorate in Chemnitz and was appointed President of the State Office for Taxes and Finances in 2011.

At the beginning of 2015, he moved to the Saxon State Chancellery as Head of the Central Department. In this function, he assumed the Chairmanship of the Commission for the comprehensive evaluation of the tasks, personnel and equipment of the Free State of Saxony. Since 10 April 2018, Thomas Popp has been Head of the Saxon State Chancellery and is responsible for the staff department "State-wide organisational planning, personnel strategy and administrative modernization."

Effective 1 August 2018, he was also appointed Chief Information Officer (CIO) of the Free State of Saxony. On 20 December 2019, Thomas Popp was appointed State Secretary and member of the Saxon State Government.

Cyber Security in Dialogue with All Segments of Society

Results of the Project „Institutionalisation of the Social Dialogue“ and Follow-up Project „Dialogue for Cyber Security“

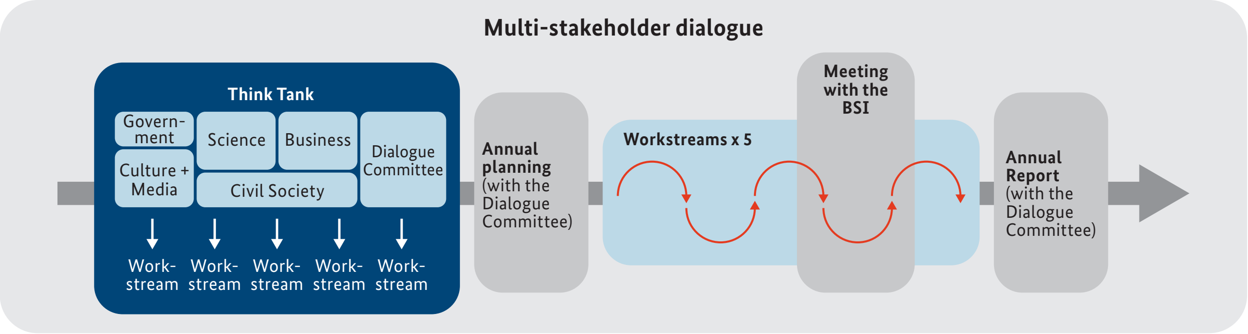
By Dr. Angelika Praus and Nora Lieberknecht, Project Group Digital Consumer Protection

The Cyber Security challenges associated with digital change can only be overcome in dialogue with all segments of society. With this in mind, the BSI has been intensifying the dialogue on Cyber Security in society as a whole since 2016 as part of a participatory multi-stakeholder approach. The project “Institutionalisation of the Social Dialogue” was completed in 2019, and the follow-up project is now to be launched.

The heart of the dialogue is the “Secure Information Society Think Tank” as a dialogue platform for players from government, science, business, culture & media and civil society. The exchange of different perspectives on Cyber Security breaks up closed discourse groups and thus promotes the sustainable development of common solution options and possibilities to take action. That is why the BSI is striving to strengthen the dialogue with organised civil society in particular and to provide impulses for its own work. The dialogue also follows the “Open Government” approach (see blog post on the 2018 Think Tank: https://opengovpartnership.de/open-government-praxis-denkwerkstatt-sichere-informationsgesellschaft).

RESULTS OF THE “INSTITUTIONALISATION OF THE SOCIAL DIALOGUE” PROJECT

Starting from the Think Tank, a core group of 15 experts from the various fields mentioned above worked on three self-chosen topics in various workshops and working meetings until the end of 2019 as part of the “Institutionalisation of Social Dialogue” project. The results were as follows:



The model shown here in simplified form shows an annual cycle of the dialogue process.

Result 1:
Mapping of players from civil society
Based on research results and qualitative interviews, the report contains a compilation of players from civil society in the field of Cyber Security as well as their main activities, objectives and networking structures.

Result 2:
Networking Day on the topic of knowledge transfer
An event was conceived and held in Berlin on 9 September 2019 that contributed to the networking of players from the fields of knowledge transfer and Cyber Security. This enabled the players to share their experiences, particularly with regard to effective activation, quality management, target audiences and formats, and create appropriate synergies.

Outcome 3:
Institutionalisation of the social dialogue
A model has been developed on how the multi-stakeholder dialogue initiated by the BSI can be deepened and made more permanent in the future (see Fig. 1).

CONTINUATION OF THE “DIALOGUE FOR CYBER SECURITY”

The multi-stakeholder dialogue is to be continued in 2020 in the follow-up project “Dialogue for Cyber Security.” The participation and multi-stakeholder model designed by the stakeholders themselves is to be implemented and made permanent over a longer period of time (up to five years).

The model will enable players from all social groups to work in a more result-oriented manner on participatory defined Cyber Security topics. In addition to the Think Tank, agile working groups, so-called “Workstreams,” in which stakeholders work together over a period of three to nine months on the topics and results they have chosen themselves, serve this purpose. By involving experts from BSI, the goal is to facilitate a continuous professional exchange.

> “The development of a framework for the discussion of critical perspectives of civil society by the stakeholders of the “Secure Information Society Think Tank” was an important step and holds potential for stronger consideration of social concerns in the security architecture.”
>
> *Daniel Guagnin is a sociologist and was a member of the working group that developed the model for deepening and stabilising the dialogue*

As the Federal Cyber Security Authority, the BSI wants to achieve greater support for the topic of IT security in society, identify new topics and needs of the various social groups in the area of Cyber Security at an early stage and incorporate impulses from the dialogue process into its own work. In particular, the annual Think Tank workshops are intended to establish a dialogue with civil society, the business world and government players in an atmosphere of trust and cooperation in order to jointly address the new Cyber Security challenges of the coming years and to shape a secure information society. ■

Further information about the project and the results here:

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

Cyber Security in Times of Emotet and Corona

Findings from the Report on the State of IT Security in 2020

In its “Report on the State of IT Security in Germany,” the BSI reports once a year on cyber threats and developments in the area of IT security. However, the current issue is not only about threats such as Emotet or critical vulnerabilities. The COVID-19 pandemic also had an impact on the IT security situation in Germany. The situation thus remains tense.

The BSI observed how attackers used malware for large-scale cyber-criminal attacks on private individuals, companies, public authorities and other institutions, but also for targeted attacks on selected victims in the reporting period June 2019 – May 2020. At the same time, the threat of data leaks has reached a new level with the disclosure of millions of patient records on the Internet.

Furthermore, several, at times critical, vulnerabilities in software products have emerged that attackers were able to exploit for malware attacks or data theft. The attackers also increasingly used the “human factor” as a gateway for attacks that use social engineering methods and simultaneously serve as a door opener for further attacks.

NEW WAVE OF MALWARE IN AUTUMN AND THE WINTER: EMOTET DOMINATES THE SITUATION

The situation was dominated by the malware Emotet, which had already proved to be particularly dangerous in the previous reporting period. It enables a cascade of further malware attacks up to targeted ransomware attacks on selected, wealthy victims. Overall, the number of new malware variants in autumn and the winter was above average (the daily increase at times was close to 470,000 variants).

MILLIONS OF PATIENT DATA FILES PUBLICLY ACCESSIBLE ON THE INTERNET

Reports of stolencustomer data were again regularly observed during the reporting period. However, theft was not the only reason for the outflow of data. Databases containing highly sensitive medical data were also discovered freely accessible on the Internet in the reporting period. In contrast to data theft, no technically complex attack was necessary here, as insufficiently secured or incorrectly configured databases were the cause of the outflow of data.

CRITICAL VULNERABILITIES IN REMOTE ACCESS

Several critical vulnerabilities were identified during the reporting period. The new vulnerabilities BlueKeep and DejaBlue in Windows Remote Desktop Protocol made many Windows systems up to Windows 10 vulnerable. The vulnerabilities allow attackers to execute arbitrary code – including malware – on the vulnerable systems. The vulnerabilities also allow for malware to spread automatically and are therefore also known as “wormable.” Microsoft has provided security updates for all affected systems.

SOCIAL ENGINEERING ATTACKS EXPLOITING THE COVID-19 PANDEMIC

Cyber criminals specialising in Internet fraud usually react quickly to socially relevant issues and trends in order to exploit them for attacks. In the course of the COVID-19 pandemic, for example, phishing campaigns, CEO fraud and attempts to defraud using IT resources were observed. For example, fraudsters managed to abuse emergency aid measures by deceptively imitating the application websites of official bodies. The corporate data that applicants had entered on the fake websites was subsequently used by the cyber criminals to impersonate applicants and fraudulently apply for aid funds. ■

IT SECURITY IN THE KRITIS HEALTHCARE SECTOR: STATUS QUO AND RECOMMENDATIONS FOR ACTION

Laboratories and hospitals in Germany are well protected against cyber-attacks and failure of their critical services. This is the result of two studies commissioned by the BSI. The studies for the KRITIS healthcare sector were developed with the aim of identifying the relevant processes of critical services and examining the status quo of information security in hospitals and laboratories in Germany. Furthermore, the studies contain recommendations for action to increase the level of protection and an outlook on the future of digitalisation within the two sectors.

They are available at:

Further information:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_stationaere_med_Versorgung.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_in_Laboren.html

The State of Cyber Security in 2020

At a Glance: Figures from the Report on the State of IT Security in Germany 2020

117.4 m new malware variants

▼ 2019: 114 m

average of **322,000** new **malware variants** every day peaking at **470,000**

76% of mail received by all government NETWORKS WAS SPAM

▶ 2019: 69% ◀

24.3 m **patient records** were accessible online according to estimates

every day up to **20,000** BOT INFECTIONS in German systems

419 CI notifications

▶ 2019: 252

▶ 2018: 145

52,000 WEBSITES

containing malware programs were blocked by web filters protecting

35,000

mails containing malware were detected in German government networks on average every month

109,000

subscribers to Bürger-CERT

▶ 2019: 105.000

▶ 2018: 100.000

around **100**

products and sites were certified by the BSI according to the

over **4,400**

members in the Alliance for Cyber Security

▶ 2019: 3,700

▶ 2018: 2,700

over **1,700**

registered **CI** facilities

just under **7m**

reports of MALWARE INFECTIONS

forwarded by the BSI to German network operators

A Look Back – a Step Forward

30 Years of the BSI: Anniversary and 17th IT Security Conference

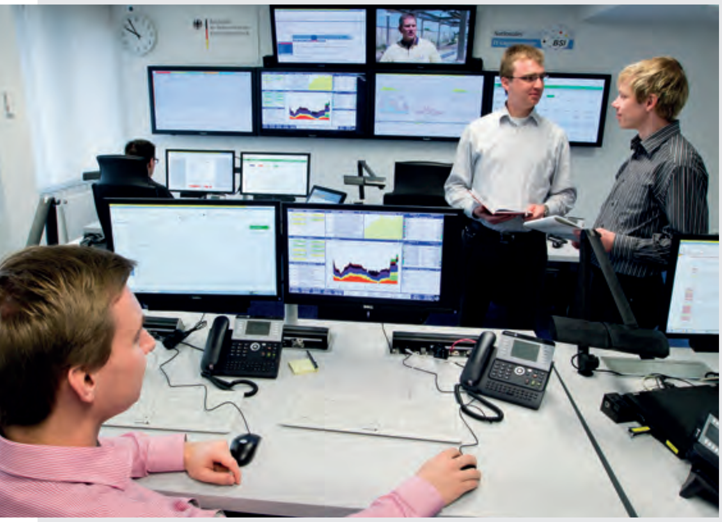
In its thirties, the Federal Office for Information Security (BSI) is still a young authority. And its area of responsibility – shaping information security in digitalisation through prevention, detection and reaction for government, business and society – can justifiably claim this attribute for itself. But thirty years is reason enough to look back.

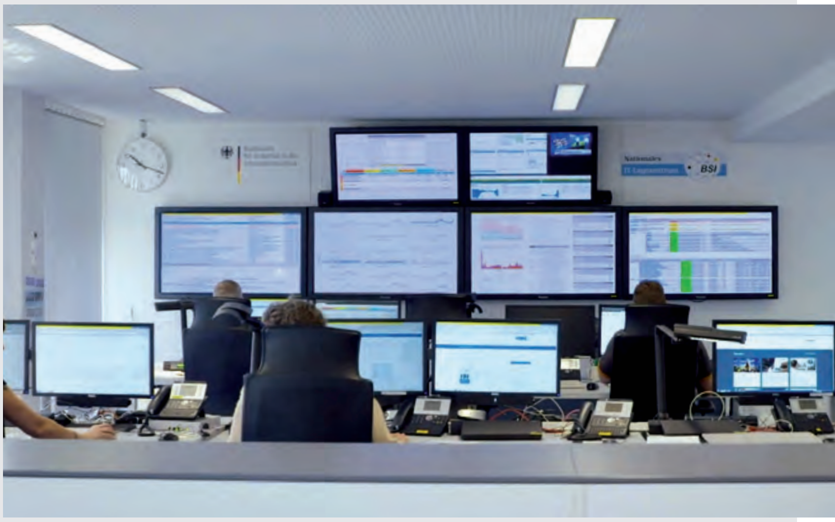
FOUNDED AS A CONSULTING AUTHORITY

When the BSI began its work on 1 January 1991 (on the basis of the BSI Establishment Act of 17 December 1990), IT security not only received a legal basis, but also a new orientation. The Act is based on a new definition of security as well as a new understanding of prevention and information policy – first formulated in the Federal Government's future IT concept from July 1989: All affected and interested parties are to be informed about the risks of information technology and possible protective measures.

The core idea that a Federal Office for IT Security should provide advice and support to all social groups was not yet a matter of course at that time. But at the latest with the beginning of the broad free use of the Internet from 1993 on, it became clear how forward-looking this approach was. IT security is now becoming a high priority government task. In order to create and promote it, to fight and reduce its threat, the state must increasingly create framework conditions, set standards and provide active support.

Not least of all, this led to a constant stream of new tasks in the years to come, including not only consulting and support, but increasingly also its own operational implementation. Founded as the central IT security service provider of the Federal Government, the protection of government networks and the securing of central network transitions have always been the most important tasks of the BSI. Since 1994, the BSI has also operated a Computer Emergency Response Team (CERT) that collects





The National IT Location Center at the BSI.

BSI FÜR BÜRGER
INS INTERNET - MIT SICHERHEIT
Bundesamt für Sicherheit in der Informationstechnik
Sicher unterwegs mit Smartphone, Tablet & Co
Tipps zum Umgang mit mobilen Geräten

BSI für Bürger Brochures
The BSI offers a total of five brochures on important topics for private users on its citizens' website, including safe use of mobile devices, important tips for using cloud services and information about the Internet of Things.

and evaluates information about vulnerabilities and new attack patterns and passes on information and warnings to the affected parties: Operational implementation of the realisation that not only the defence against malicious software and the indication of vulnerabilities are important, but also the reaction to IT security incidents.

SOLID LEGAL FRAMEWORK

With the BSI Act, which was amended in 2009 by the German Federal Government's Act to Strengthen Security in Information Technology, the BSI was able to develop binding security standards for the procurement and use of IT for Federal authorities. It has become the central reporting office for IT security within the Federal Administration, in order to ensure the Federal Government's ability to make decisions and act, especially in the event of IT crises of national importance, by providing processed information and competent analyses. And it established an IT crisis management system for the Federal Administration as a kind of early warning system that enables the creation of situation pictures, defines crisis reaction processes and backs them up with exercises.

Once again – and decisively – the tasks and powers of the BSI were expanded by the IT Security Act, which came into force in July 2015. With binding minimum requirements for IT security, flanked by an obligation to report significant IT security incidents, the law aims above all to improve the protection of critical infrastructures (KRITIS) and to increase network security in those sections whose failure or impairment of supply services would have dramatic consequences for the economy, state and society in Germany. KRITIS operators must therefore regularly prove to the BSI that they comply with state-of-the-art IT security (§ 8a BSIG). If security deficiencies are discovered, the BSI may, in agreement with the supervisory authorities, order their elimination.

The BSI is also the central reporting office for the IT Security of Critical Infrastructures (according to § 8b BSIG). They must report significant disruptions of their IT to the BSI if they could have an impact on the availability of critical services. The BSI evaluates and analyses these reports and correlates them with other reports and findings from other sources.

This results in a situation picture, on the basis of which, for example, short-term warning and alarm messages as well as recommendations for action for those affected can be created. Conversely, the BSI collects and evaluates all information relevant to the defence against attacks on the IT security of critical infrastructures and forwards it to the operators and the responsible (supervisory) authorities. The operators thus receive information and know-how and can benefit from the BSI's evaluation of reports from all operators and many other sources.

29th Cyber Security Day of the Alliance for Cyber Security
With a new event concept, the Alliance for Cyber Security (ACS) and the German Association of Chambers of Industry and Commerce (DIHK) invited interested parties to attend the 29th Cyber Security Day in Berlin on 26 September 2019. While many issues related to Cyber Security can be resolved on an individual basis, it is often much easier to learn from the experiences and insights of others.

In two ordinances for the implementation of the IT Security Act, it was regulated in detail which companies from the KRITIS sectors energy, information technology and telecommunications, transport and traffic, health, finance and insurance as well as water and food fall under the IT Security Act.

As solid as this legal framework is, the development of digitalisation cannot be paused. The current draft of an IT Security Act 2.0 was created from the implementation of the IT Security Act and against the backdrop of the current threat situation. It provides for new obligations for the operators of critical infrastructures, but also new tasks for the BSI such as digital consumer protection and a mark for the security of IT products. Both are intended to raise awareness of Cyber Security and to significantly increase the level of security.

COOPERATIVE DESIGN OF CYBER SECURITY

Secure digitalisation and increasing the level of information security is a task for society as a whole that requires intensive cooperation between the various players. As the Federal Cyber Security Authority, the BSI shapes information security in digitalisation through prevention, detection and reaction with a distinctive cooperative approach to protect the government, politics, society and business. It relies on close and equal cooperation between all players and makes its comprehensive, independent and neutral expertise available.

In this way, Germany has a functioning cyber defence from a single source. This is particularly evident where the BSI has been able to develop new target audiences and offer new information and support in the context of its expanding responsibilities beyond its original task:

In the KRITIS area, the BSI cooperates with the KRITIS operators, their associations and the responsible government agencies in the public-private partnership UP KRITIS, in addition to its tasks under the IT Security Act. The implementation plan (UP) addresses eight of the nine critical infrastructure sectors. At the Federal level, the UP BUND addresses the Government and Administration sector. The necessary regulations for Federal States and municipalities are made by the Federal States.

The Alliance for Cyber Security, which was initiated in 2012 together with the ICT industry association Bitkom,

Das BSI als die nationale Cyber-Sicherheitsbehörde
gestaltet Informationssicherheit in der Digitalisierung
durch Prävention, Detektion und Reaktion
für Staat, Wirtschaft und Gesellschaft.

16th IT Security Conference
The BSI brought together around 700 IT security experts in 2019.

aims to strengthen the resistance of small and medium-sized enterprises in particular to cyber-attacks. This is achieved, among other ways, by providing practicable IT security recommendations for SMEs by the BSI and partners of the alliance. More than 4,400 institutions now belong to the Alliance, including more than 140 partner companies and nearly 100 multipliers.

With the website www.bsi-fuer-buerger.de and the free warning and information service “Bürger-CERT,” the BSI also makes its findings on the Cyber Security situation available to private users for the protection of their IT systems and data. With the Facebook page www.facebook.com/bsi.fuer.buerger and the Twitter channel www.twitter.com/BSI_Presse, the BSI is also represented in social networks.

On the basis of its in-depth technical expertise, the BSI already has an integrated value chain from consulting to the development of technical security solutions, defence against attacks on Cyber Security to regulation and certification. But it is also true that, analogous to the increasing importance of Cyber Security in a highly networked society, the future challenges of the BSI are certainly no less than those at the time of its founding. ■

17TH GERMAN IT SECURITY CONFERENCE

On 2 and 3 February 2021, the BSI will hold the 17th German IT Security Conference that is held every two years. The IT Security Conference will take place in hybrid form for the first time: The moderation and speaker presentations will take place live on site, and the conference participants will take part virtually. For two days, participants from administration, business and science will exchange views on current trends and perspectives in IT security. The conference is a fixed appointment in the event calendar of the IT security industry and beyond. Its goal is to illuminate the topic of IT security from different perspectives, to present and further develop solutions. Once again, there will be a large number of creative, practical and comprehensible contributions, from which a programme of events will be composed that covers the entire spectrum of Cyber Security. The Parliamentary State Secretary Prof. Dr. Krings (Federal Ministry of the Interior) has already agreed to be a speaker at the conference. On the occasion of the 30th anniversary of the BSI, next year’s conference will include the anniversary celebration in the first day of the event.

The Year 2020 for the BSI

Review

The BSI and the VDA: Together for more Cyber Security in cars
The BSI and the German Association of the Automotive Industry (VDA) will be working together closely on Cyber Security issues in the future. A joint declaration of intent was signed by VDA President Hildegard Müller and the President of the BSI Arne Schönbohm in Berlin.

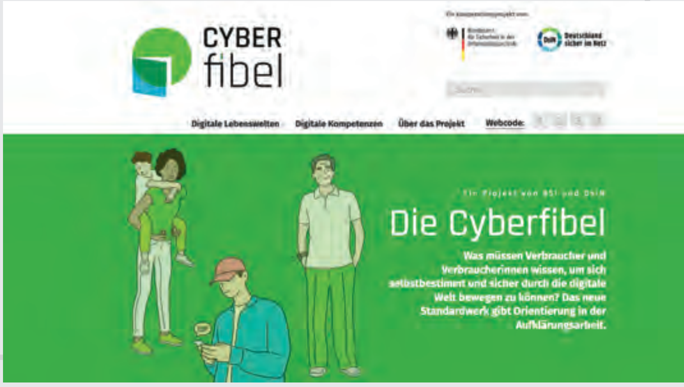
Security requirements for telecommunications networks published
The Federal Network Agency published the latest draft of the catalogue of security requirements for operating telecommunications and data processing systems and for processing personal data today. The catalogue was prepared in consultation with the BSI and the Federal Commissioner for Data Protection and Freedom of Information.

Threat prevention moves further into the foreground: Interdepartmental cooperation between Kommando CIR and the BSI
BSI employees strengthen the Blue Team during the Locked Shields cyber defence exercise.

The BSI and Consumer Organisations strengthen digital consumer protection
Together for a secure digital world – the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband e.V., vzbv) and the BSI have agreed on this goal. vzbv chairman Klaus Müller and the President of the BSI Arne Schönbohm signed a joint agreement on this topic (Memorandum of Understanding) on 4 June.

More Cyber Security in aviation: The BSI and the EASA agree on a strategic cooperation
Modern aircraft are digitally networked, flying high-performance computers. For a smooth flight, cyber security must be considered in addition to basic flight safety. The common goal of the BSI and the European Union Aviation Safety Agency is to increase Cyber Security in international aviation on a sustainable basis.

Information offers and services for citizens
The Cyberfibel is a cooperation project of the Federal Office for Information Security (BSI) and Deutschland sicher im Netz e. V..



CYBER fibel

Digitale Lebenswelten | Digitale Kompetenzen | Über das Projekt | Webcode:

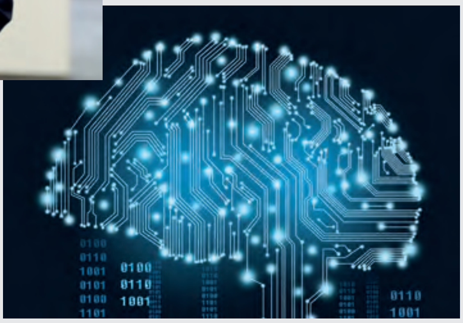
Ein Projekt von BSI und DsiN

Die Cyberfibel

Was müssen Verbraucher und Verbraucherinnen wissen, um sich selbstbestimmt und sicher durch die digitale Welt bewegen zu können? Das neue Standardwerk gibt Orientierung in der Aufklärungsarbeit.

#CyberConference2020
The BSI and the Federal Ministry of the Interior are organising the Cyber Security Conference on the occasion of the German EU Council Presidency.

The BSI as (co-)designer in the field of digital healthcare
One topic during the visit by Health Minister Jens Spahn: How much should hospitals invest in their information security? The answer can now be found in the Hospital Future Act (Krankenhauszukunftsgesetz), which provides for at least 15 percent of the funding applied for to be used for measures to improve information security.



The BSI publishes study on the security of blockchain applications
The BSI has had around 300 block chain applications evaluated as part of a market analysis. The study was commissioned by the Forschungszentrum Informatik (FZI) in Karlsruhe.

The BSI team wins all of the prizes at the CHES Challenge
The BSI participated once again in the side channel competition in 2020 with a team of eight employees and won all of the prizes that were awarded.

IT SECURITY IN PRACTICE

How Secure is the Company Car?

New IT-Grundschutz Module „General Vehicle“ Highlights IT Security in Vehicles

By Daniel Gilles, Section BSI Standards and IT-Grundschutz

Digital assistance and infotainment systems have become an integral part of modern vehicles such as conventional cars, trucks, ships or airplanes. This results in new risks for the IT security of the vehicles, which the BSI addresses in its new IT-Grundschutz module "General vehicle."

For more than 25 years, the BSI has been offering a proven methodology for dealing efficiently with the issue of IT security with its IT-Grundschutz. The IT-Grundschutz Compendium, which is continuously developed as a "living tool" is at the focus of the practical work. Around 100 specialised texts deal with different aspects and facets of IT security in ten so-called IT-Grundschutz components. They describe dangers and requirements, name those responsible in companies and authorities and thus enable well-founded security considerations. They also provide answers to questions like: What requirements for IT security are important? What regulations must be defined?

IT-Grundschutz is constantly being further developed, trends are evaluated and topics added. The new IT-Grundschutz module "General vehicle," which considers the IT security of vehicles and thus takes the rapid development in the field of vehicle IT into account is a result of this updating.

SECURING THE MOBILE OFFICE INSIDE THE VEHICLE

For all vehicles – whether on roads, on the water or in the air – IT security must also be taken into account, in addition to aspects of conventional vehicle safety, at an early stage when new equipment is used. Nowadays, a freight forwarder has information on his customers, such as contact details or scope of delivery, inside the trucks he uses. A sales employee has a mobile office with a laptop and a smartphone in his car that is connected to the IT inside the vehicle. Vehicles that are used for business purposes and come from the factory equipped with considerable IT equipment are exposed to special risks. Figure 1 provides an overview of the possible dangers.

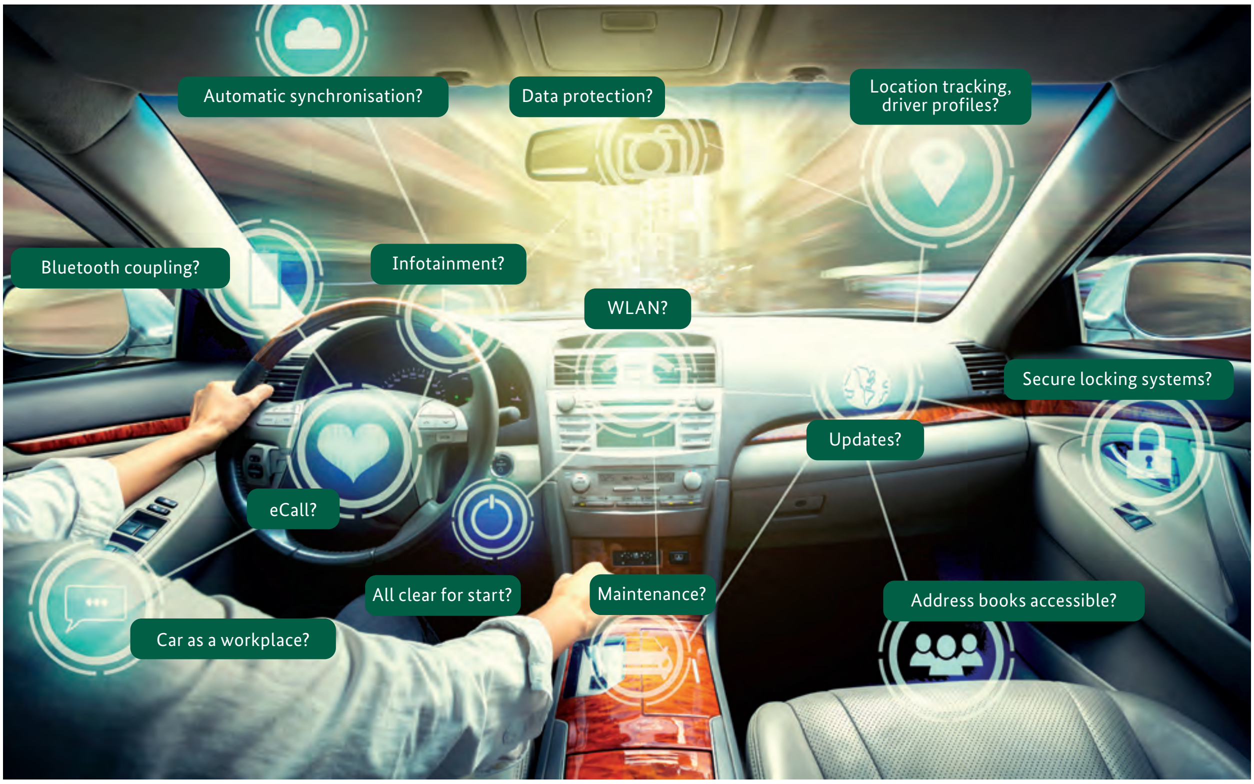


Figure 1: Risks for IT security inside cars

ONE TOPIC – MANY SYNERGIES

Specialists from the Command Cyber and Information Space of the German Armed Forces, from the Federal and State Police as well as from the fire department have dealt with the same questions regarding secure vehicle IT. Together with these experts, the BSI has founded an interdisciplinary working group to develop the new module “General vehicle.” This module can be used for all types of vehicles with engines and vehicle cabs that generally travel on roads, in the air, on water and at sea. The module shows how a vehicle can be used as a secure mobile working environment and how the IT integrated into the vehicle can be secured. For this purpose, organisational requirements for vehicle deployment as well as vehicle selection and procurement are especially important, since technical protection of the IT components integrated into the vehicle is usually only possible to a limited extent. The locking systems of the vehicles is a good example of this. Already during selection of the vehicles, care should be taken to ensure that the vehicles have adequately secure locking systems. If vehicles in the inventory are used that have insecure locking systems, security can in many cases be guaranteed by organisational measures. Vehicles with keyless locking systems that can be bypassed by relay attacks is just one example. In most cases, it is sufficient to deactivate the keyless function of the locking system to prevent relay attacks.

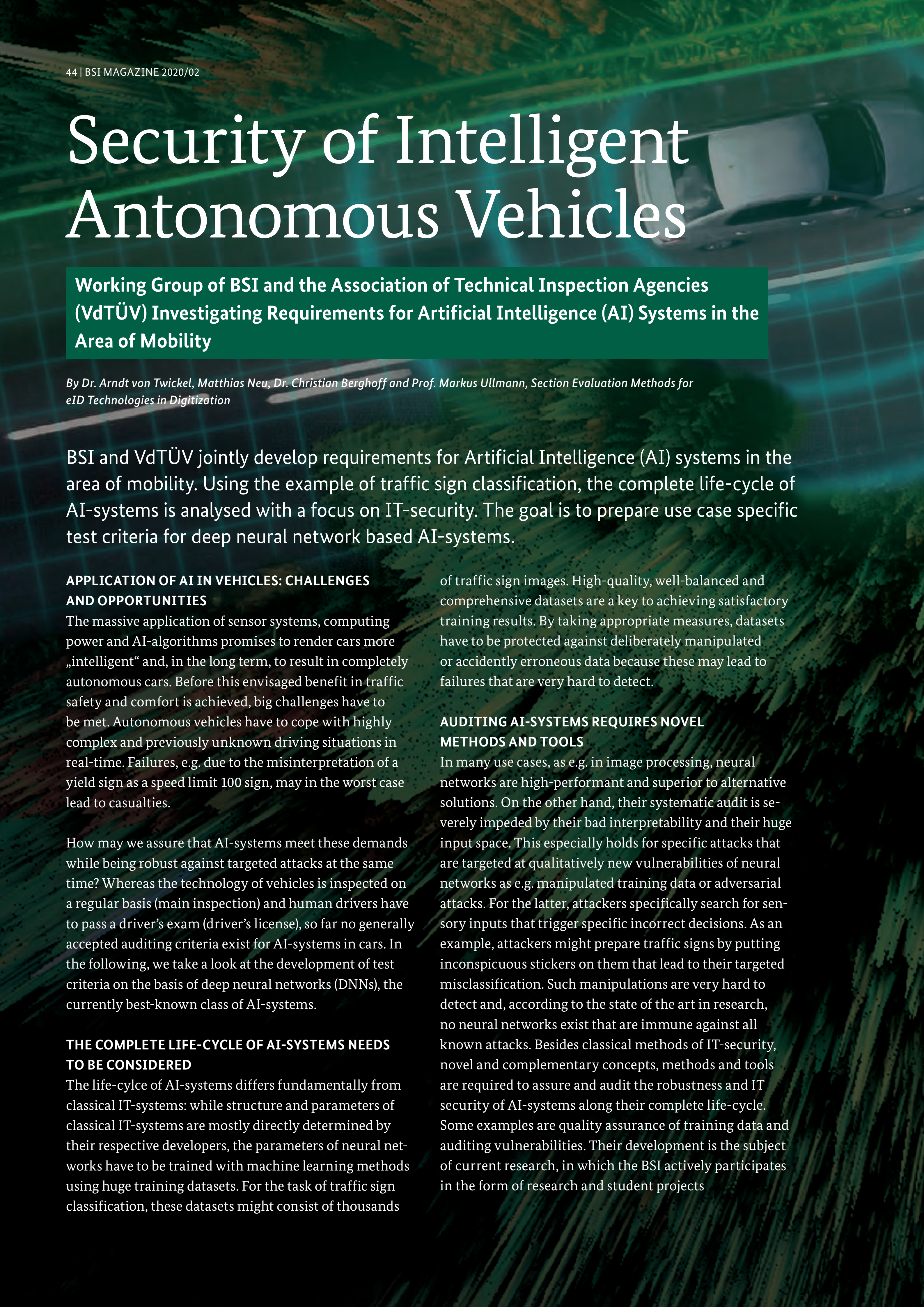
FROM A DRAFT TO THE IT-GRUNDSCHUTZ COMPENDIUM 2021

The new IT-Grundschutz component forms the initial starting point for the broad range of topics of IT security of vehicles. Due to the increasing spread of IT in vehicles of all kinds, it is conceivable that the first IT-Grundschutz component will be supplemented in the future to include components on other topics. In the past, it has proven to be a good idea for users and experts to first create a user-defined module for specific application scenarios, such as special vehicles. This is published on the BSI website for technical discussion and further development. Through this procedure, the IT-Grundschutz Compendium is constantly being expanded to include further current topics.

The BSI is happy to receive feedback on the new IT-Grundschutz component and further suggestions on the topic of IT Security for vehicles at grundschutz@bsi.bund.de. ■

More information:

https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html



Security of Intelligent Antonomous Vehicles

Working Group of BSI and the Association of Technical Inspection Agencies (VdTÜV) Investigating Requirements for Artificial Intelligence (AI) Systems in the Area of Mobility

By Dr. Arndt von Twickel, Matthias Neu, Dr. Christian Berghoff and Prof. Markus Ullmann, Section Evaluation Methods for eID Technologies in Digitization

BSI and VdTÜV jointly develop requirements for Artificial Intelligence (AI) systems in the area of mobility. Using the example of traffic sign classification, the complete life-cycle of AI-systems is analysed with a focus on IT-security. The goal is to prepare use case specific test criteria for deep neural network based AI-systems.

APPLICATION OF AI IN VEHICLES: CHALLENGES AND OPPORTUNITIES

The massive application of sensor systems, computing power and AI-algorithms promises to render cars more „intelligent“ and, in the long term, to result in completely autonomous cars. Before this envisaged benefit in traffic safety and comfort is achieved, big challenges have to be met. Autonomous vehicles have to cope with highly complex and previously unknown driving situations in real-time. Failures, e.g. due to the misinterpretation of a yield sign as a speed limit 100 sign, may in the worst case lead to casualties.

How may we assure that AI-systems meet these demands while being robust against targeted attacks at the same time? Whereas the technology of vehicles is inspected on a regular basis (main inspection) and human drivers have to pass a driver's exam (driver's license), so far no generally accepted auditing criteria exist for AI-systems in cars. In the following, we take a look at the development of test criteria on the basis of deep neural networks (DNNs), the currently best-known class of AI-systems.

THE COMPLETE LIFE-CYCLE OF AI-SYSTEMS NEEDS TO BE CONSIDERED

The life-cylce of AI-systems differs fundamentally from classical IT-systems: while structure and parameters of classical IT-systems are mostly directly determined by their respective developers, the parameters of neural networks have to be trained with machine learning methods using huge training datasets. For the task of traffic sign classification, these datasets might consist of thousands of traffic sign images. High-quality, well-balanced and comprehensive datasets are a key to achieving satisfactory training results. By taking appropriate measures, datasets have to be protected against deliberately manipulated or accidently erroneous data because these may lead to failures that are very hard to detect.

AUDITING AI-SYSTEMS REQUIRES NOVEL METHODS AND TOOLS

In many use cases, as e.g. in image processing, neural networks are high-performant and superior to alternative solutions. On the other hand, their systematic audit is severely impeded by their bad interpretability and their huge input space. This especially holds for specific attacks that are targeted at qualitatively new vulnerabilities of neural networks as e.g. manipulated training data or adversarial attacks. For the latter, attackers specifically search for sensory inputs that trigger specific incorrect decisions. As an example, attackers might prepare traffic signs by putting inconspicuous stickers on them that lead to their targeted misclassification. Such manipulations are very hard to detect and, according to the state of the art in research, no neural networks exist that are immune against all known attacks. Besides classical methods of IT-security, novel and complementary concepts, methods and tools are required to assure and audit the robustness and IT security of AI-systems along their complete life-cycle. Some examples are quality assurance of training data and auditing vulnerabilities. Their development is the subject of current research, in which the BSI actively participates in the form of research and student projects

FORMULATING REQUIREMENTS FOR AI-SYSTEMS NECESSITATES CONSIDERING CONCRETE USE-CASES

Along the life-cycle of AI-systems, the AI-working group of the BSI and VdTÜV has initially worked out generalized requirements, e.g. with respect to data quality and appropriate network models, and in so doing has taken diverse perspectives into account, such as robustness, IT-security and interpretability. Subsequently, the resulting requirements were adapted for an application-relevant AI system which was chosen to be as simple as possible: a system for traffic sign classification. This way, it was established that the generalized requirements could be transferred either directly or with minimal adaptions to the use-case specific requirements. Further steps will include 1. testing and refining the requirements specifically developed for traffic sign classification systems in practical projects; 2. adapting the generalized requirements for AI-systems to further, qualitatively different, use cases to verify their transferability; 3. investigating interaction effects between multiple interacting (AI-)systems and 4. working out audit criteria that prove that specific requirements are met. Findings of the BSI-VdTÜV AI-working group are first discussed with experts from academia and industry and then transferred to national and international standardization committees such as DIN and ETSI. The long-term goal is to enable the auditing of autonomous vehicles, consisting of multiple subsystems, as afoundation for their safe and secure operation on the road. ■

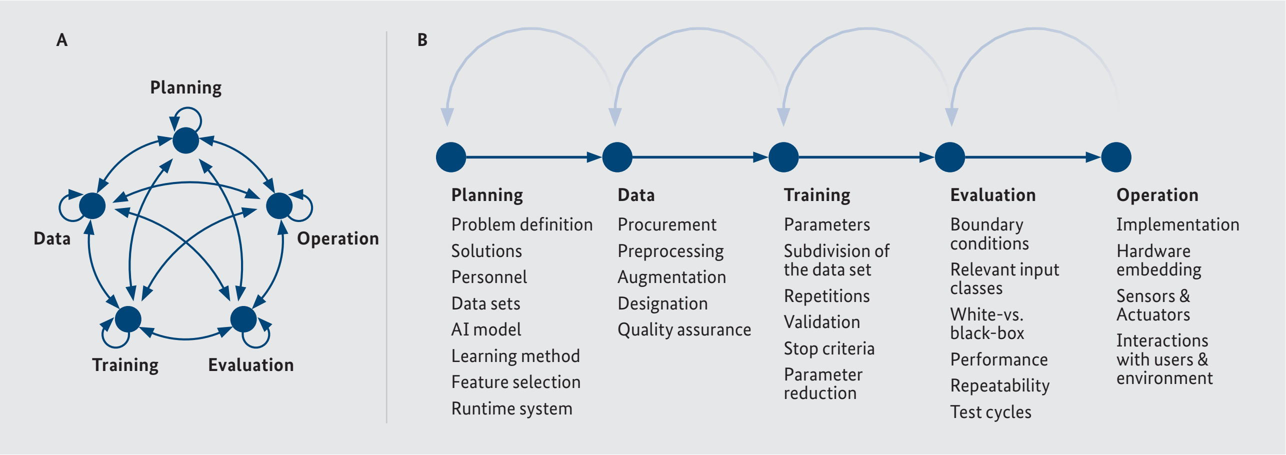


Figure 1: Life-cycle of an AI-system
The life-cycle of an AI-system may be subdivided into multiple phases: planning, data, training, evaluation and operation. (A) In reality the development of an AI-system is non-sequential, meaning that it jumps back and forth between different phases. Often, it is additionally dependent on the intuition and experience of the developer. The developer tries to find the quickest route to a deployable AI-system with the desired properties. (B) For the analysis of the life-cycle and for the development of the requirements, a sequential presentation is helpful. For each phase, important functional components are listed. Further important components, e.g. from the perspectives of robustness, data safety and user acceptance, are not mentioned here.

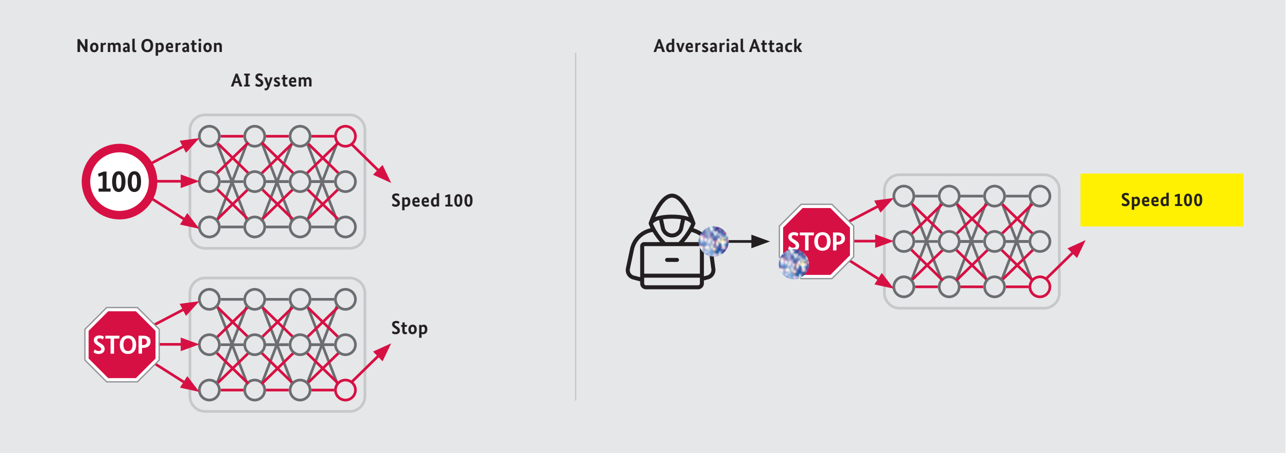
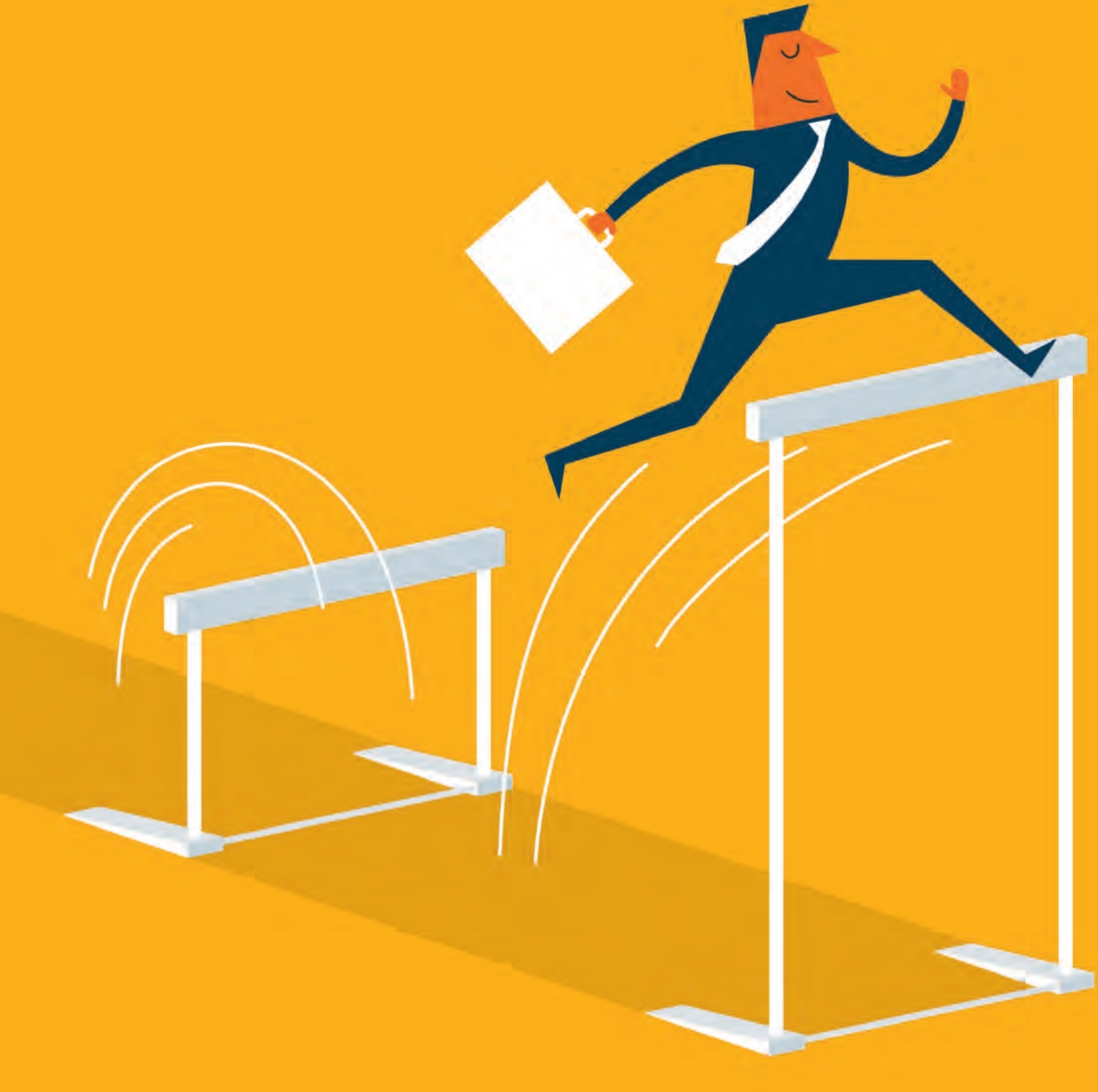


Figure 2: Adversarial attack on traffic sign classification
For input data that are well represented in the training dataset, an AI system usually takes the desired decision in a robust way as shown on the left side and schematically for the traffic signs "Stop" and "100". Attackers performing adversarial attacks make use of the huge input space of AI-systems, which can in no way be completely covered by a practically usable data set. Within this huge input space, attackers search for inputs that lead to targeted misclassifications. In the schematic example on the right, an attacker has computed the pattern for a sticker which will lead to a wrong classification of the stop sign as speed limit 100 sign.

COVID-19 Pandemic: A Baptism of Fire for the New Government Networks

By Dr. Lothar Eßer, Section Security of Government Networks – Business Continuity Management and Applications



The current pandemic situation due to COVID-19 also has an impact on federal information technology applications and infrastructures, of which the federal networks (NdB) deserve special mention.

The federal networks (NdB) replaced the Information Network Berlin-Bonn (IVBB) as the interdepartmental, central infrastructure on July 1st 2019. The IVBB had previously successfully ensured communication between the federal ministries, their subordinate departments, the German Bundestag and the federal courts for 20 years. The federal networks are also equipped with specially secured transitions to external networks in order to enable employees of the above-mentioned authorities to communicate securely, e. g. by telephone or Internet research, and to communicate securely with colleagues in the states, of course.

The Federal Agency for Public Safety Digital Radio (BDBOS) is responsible for the operation, and the Federal Office for Information Security (BSI) is in charge of the security of the federal networks. Deutsche Telekom Business Solutions GmbH (DTBS) is the current operator. All three institutions work together closely and constructively and ensure a fast and transparent flow of information in order to maintain the stability and security of the government networks at a high level at all times.

The federal networks serve around 650 different properties throughout Germany, with a focus on Bonn and Berlin. The well over 100,000 employees, who mainly carried out their work before the in the properties of their respective authorities, generally make an average of 100,000 interagency telephone calls per day via the central infrastructure. Between 2 and 5 Gbit/s in both directions are generated at the central Internet access points, and more than 1,000,000 e-mails pass through the central e-mail system every day.

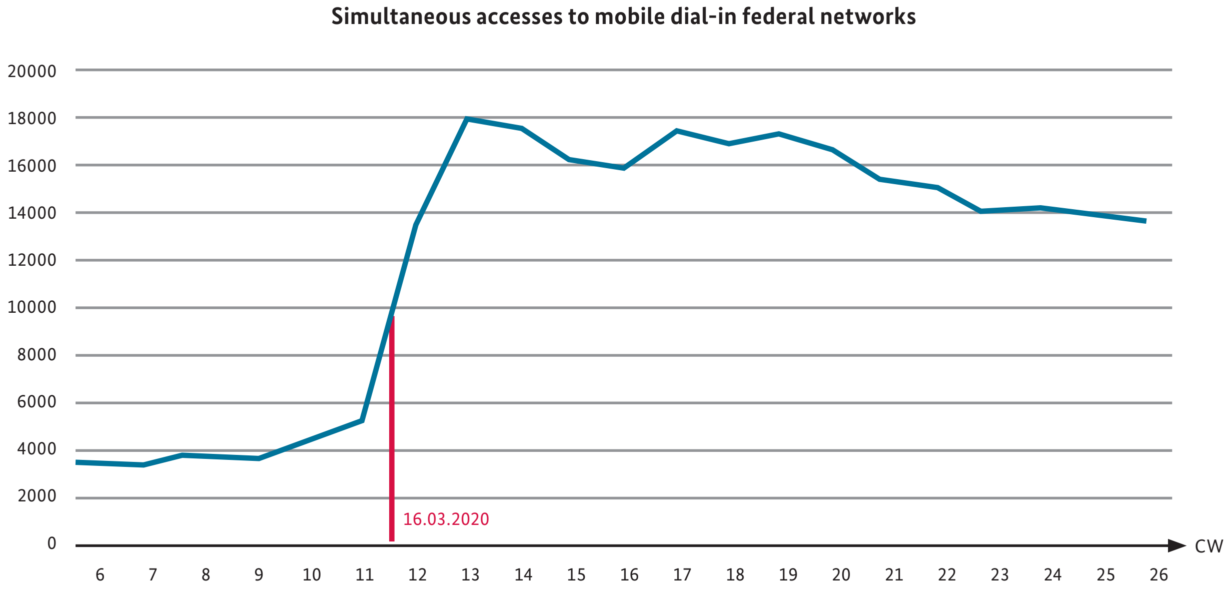
When initial reports about the spread of the COVID-19 virus in China and its impact worried the world earlier this year, the situation was monitored closely by the three institutions responsible for the federal networks (BDBOS, BSI and DTBS). Initially the situation seemed to be under control and the WHO was reluctant to admit the threat of a global pandemic. Nevertheless, the DTBS started to take preventive measures. The operational teams were divided into groups in order to minimise individual, personal contacts outside these groups. All groups also had sufficient expert knowledge. This was one of the reasons why it has been possible to prevent a large number of operating personnel from being absent due to infection with the virus or in quarantine. The further spread in Italy and the spread of the virus in the Heinsberg district alarmed all three parties involved. The BDBOS and BSI then analysed the technical situation in the central infrastructure in close cooperation, assuming that a larger number of employees had to do their work from their workplace at home, e. g. due to an ordered quarantine.

The analysis led to the following result:
The technology used in the central infrastructure is dimensioned and secured by redundancy measures in such a way that sufficient reserves are available for the communication load mainly generated in the authorities, taking economic efficiency into account. However, the analysis also showed that, assuming a move of office work to working at home, bottlenecks would arise in the areas of mobile access, telephone and video conferencing and telephony in the public network. The BDBOS and BSI immediately initiated the first technical measures with the DTBS to counteract these bottlenecks, even before the school closures became known, and initiated the necessary procurements to counteract any foreseeable supply bottlenecks.

In mid-March, things suddenly and unexpectedly took a turn for the worse, especially with unprecedented severity, with school closures nationwide and further precautionary measures decided by the Federal and State Governments against the spread of the COVID-19 virus. As a consequence, many government employees moved to their workplaces at home and carried out their official duties from there.

Figure 1 shows that the simultaneous use of one of the most important mobile services suddenly increased from around 4,000 to over 9,000 on 16 March 2020, the first day of school closures. In the days and weeks that followed, the number of concurrent users continued to rise to over 16,000.

Not all of the previously initiated measures had been fully implemented at the time of the school closures. As a result, there were restrictions in the first one to two weeks after 16 March 2020, especially on telephony to the public network and on conference calls. All parties involved



further intensified their efforts to eliminate the restrictions as soon as possible.

Overall, the capacity of the main mobile service, among other services, had been quadrupled in a short period of time. Connections to the public telephone network had been more than doubled. The number of simultaneous participants in conference calls were increased by a factor of 22. The redundancy of Internet access was improved and the bandwidth at one site increased by 6 Gbit/s. The possibilities of mobile access via smartphone were also increased by about 50%. Other new mobile services will also be available soon.

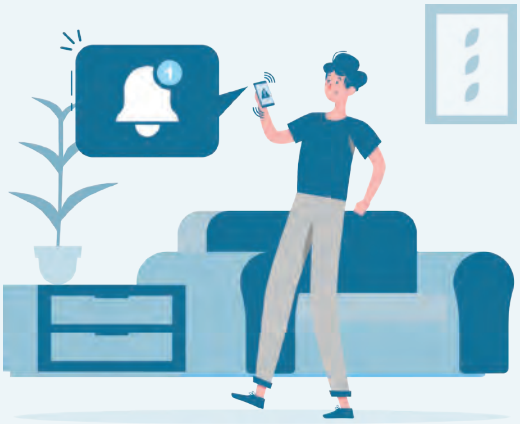
Increasing capacity in the area of video conferencing solutions proved to be the greatest challenge. The relocation of a large number of workers/employees to the workplace at home suddenly increased the need to conduct video conferences with colleagues or external partners directly from the workplace. It should be noted that video conferences within the federal networks must be suited for classified information.

Most authorities operate their in-house networks connected to the federal networks independently. They are therefore not part of the central infrastructure, as was previously the case with the IVBB. The authorities are therefore equally faced with the challenge of providing their staff with appropriate video conferencing solutions. Due to the high demand and lack of capacity at the same time, some authorities implement their own solutions or use solutions from cloud providers.

The BDBOS, with the support of the BSI, intensified its efforts to significantly expand the current range of secure video conferencing solutions in the federal networks. Improvements in the technology of classified information-compliant solutions as well as the establishment of a system for normal protection requirements for up to 1,000 simultaneous participants have already been reported

SUMMARY

Nearly half a year after the launch of the federal networks, the new government networks have already survived their first test in a baptism of fire. This called for numerous extensions to be implemented within only a very short period of time. These had become necessary due to a significant change in usage behaviour overnight during the COVID-19 pandemic. To this end, all those involved have worked closely and constructively together and can contribute to the knowledge and experience gained in recent weeks to the new challenges now to be expected, as neither the COVID 19 pandemic nor the associated measures in the Federal Government networks have come to an end. Furthermore, the main firewall as well as the network and authority connection capacities with their security measures must be adapted in order to enable secure applications with high data rates, such as video conferencing solutions, for every workplace, whether in the office or at home. ■



BSI Basic Tip

Already Updated Today?

Update, Patch, Refresh or Bugfix – Why Regular Updates Are So Important

Doesn't it seem as if update requests usually appear when we are doing important work on the computer or smartphone? As annoying as these requests sometimes are – updates protect us. Operating systems for PCs and laptops, apps on smart TVs, software on smartphones or even the virus protection program – they all only offer computer malware the smallest possible target if they are kept up to date. This makes it all the more alarming that only a quarter (25 percent) of Internet users in Germany activate the automatic installation of updates. This is the result of the "Digital Barometer 2020" survey conducted by the German Federal Office for Information Security (BSI) and the initiative Police Crime Prevention of the Federal States and the Federal Government (ProPK). 57 percent of those surveyed rely on measures such as virus protection programmes or firewalls. However, regular updates offer a protective effect that should not be underestimated and thus represent an important preventive measure. They close security gaps, eliminate bugs in the operating system and add new functions. For instance, updates prevent an antivirus programme from having to detect and block or remove malware that has already been infiltrated.

Ignoring updates can have unpleasant consequences. Fraudsters can exploit known security gaps to install malware. The effects can be significant: Malware can steal, delete or encrypt data and manipulate programmes. This can lead to the complete loss of data or the misuse of passwords and bank data.

Prominent example: In April 2017, the malware WannaCry infected tens of thousands of computers around the world and encrypted files that were saved on them. This happened because the Windows operating systems had not been updated to the latest version. Even today, systems without this update are still at risk from WannaCry. Updated systems, however, were and still are untouchable for this malware.

HOW TO KEEP TRACK OF IMPORTANT SOFTWARE UPDATES

1. Get an overview of the programmes you use on your PC, laptop, tablet and smartphone! Check which products you can set up automatic update services for and always enable automatic updates!
2. Make it a rule for yourself to follow notes on updates and don't click them away!
3. Create an overview of the programmes for which you must pay attention to updates on your own! Inform yourself regularly about updates – by subscribing to newsletters, for example.
4. Install updates as soon as they are available!

Related links:

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

9-Point Plan for a Digital Germany

An Interview with Dr. Markus Richter, State Secretary at the Federal Ministry of the Interior, Building and Community and Federal Government Commissioner for Information Technology

■ **State Secretary Dr. Richter, you published a "9-Point Plan for a Digital Germany" shortly after you took office, with which you intend to promote digitalisation in Germany. What are the key points of this plan?**

We want to make tangible progress in the area of digitalisation in the months ahead. To this end, we have compiled what we consider to be nine key points in a priority plan based on the three pillars of digitalisation in the BMI: Digital Society, Digital Administration and Cyber and Information Security. I am convinced that we will make significant progress in digitalisation in Germany by implementing this plan.

Our goal is also to convince people of the added value of digitalisation. We will only succeed in doing this if we make its benefits tangible as quickly as possible.

Therefore, we are prioritising projects that produce concrete results: In the coming months, we will be working hard on projects such as the implementation of the German Online Access Act (Onlinezugangsgesetz), but also on very concrete milestones such as the creation of a digital academy to train administrative staff, optimisation of online ID cards, the nationwide introduction of the e-bill and e-files, and the evaluation and updating of the Cyber Security Strategy from 2016.

■ **Where do you see the challenges in the area of Cyber Security?**

The challenges for Cyber Security arise in particular due to the increasing digitalisation of all areas of life and the constant technological progress in general.

We are making significant progress in strengthening Cyber and Information Security, but are constantly confronted with a large number of new developments that naturally also entail risks. New technologies such as wearables, i.e. intelligent electronic devices that are worn on the body, in particular the Smart Watch, are permeating our everyday lives. The constant Internet connection and GPS tracking of these devices opens up new possibilities for criminal intent, such as violating users' privacy.

We must also note that malicious programmes are becoming increasingly sophisticated and cyber-attacks are becoming more targeted. For example, Emotet, a malicious programme that has been known for a long time, is constantly being adapted and equipped with new capabilities by the attackers. Emotet is distributed through spam campaigns and poses an acute threat to users.

Among other things, the malware reads contact relationships and e-mail contents from the mailboxes of infected systems. The perpetrators then use this information to spread the programme further. Once a system is infected, Emotet downloads additional malware. For home users, an infection can mean the loss of important data.

I also see another major challenge in maintaining and strengthening the digital sovereignty of Germany and Europe. Currently, public administration is highly dependent on individual IT providers. This can also lead to risks such as limited information and data security.
It is therefore necessary to further strengthen digital sovereignty and thus our own ability to act in the digital arena, and we are tackling this issue.

■ **How can the BSI, in its role as the designer of information security in digitalisation, help you implement your 9-point plan?**

As the Federal Cyber Security authority, it is the task of the BSI to make Germany digitally secure. The BSI has been at our side now for nearly 30 years. It provides versatile support to ensure the highest level of IT security for the population. So, let me begin by thanking you for this. Our goal is to make it easier for people to access digital

> “I see a great challenge in maintaining and strengthening the digital sovereignty of Germany and Europe.”

living spaces securely. Citizens and companies alike must feel secure when they use the administrative services digitised under the Online Access Act, for example. And we need the BSI for this. With regard to the Online Access Act, I am thinking in particular of your security consulting services.

We have anchored a number of topics in our 9-Point Plan that must be implemented directly by the BSI. Let’s just take the topic of digital consumer protection, for instance, which is to become a task of the BSI with the IT Security Law 2.0.

In this context, we plan to introduce a uniform and voluntary IT security label. This label will make the IT security of products in the consumer segment transparent and comprehensible for citizens for the first time. The basis for this is initially provided by the technical guidelines issued by the BSI. The first technical guideline has already been issued by the BSI for broadband routers. The goal is for citizens to be able to use this “digital package insert” to obtain information about the IT security of the products they purchase ■

Brief Profile Dr. Markus Richter

Dr. Markus Richter is State Secretary at the Federal Ministry of the Interior, Building and Community and Federal Government Commissioner for Information Technology. Among other things, the lawyer has been head of the IT section at the Federal Office of Administration, Head of the Department for Infrastructure and IT and CIO at the Federal Office for Migration and Refugees and Vice President at the Federal Office for Migration and Refugees. Dr. Markus Richter was born in Münster, Westphalia, in 1976. He has two children.

How Secure is Contactless Payment via Near Field Communication?

The BSI Subjected Payment Cards and Terminals to Comprehensive Tests

By Sabine Mull and Rainer Schönen, Section Cyber Security in the Public Health and Financial Services Sectors

Many users of checking account and credit cards equipped with a corresponding NFC chip are worried that contactless bank cards can be read not only at the cash terminal, but quasi always and virtually anywhere. There are repeated reports in various media that the function for contactless payment in checking account cards and credit cards represents a security risk. Video clips show how a small mobile payment terminal can be used to debit amounts of up to EUR 50 from the accounts of unsuspecting passers-by without authorisation. All they need to do is hold the terminal up to someone's pant pocket or handbag and the theft has already occurred.

HOW REAL IS THIS DANGER?

First of all, we should keep in mind that criminals must link an account to the payment terminal in order for money to be withdrawn at all. To open an account, however, they have to identify themselves in accordance with the standards of the Money Laundering Act, so this at least poses an initial hurdle.

There are also technical aspects to be considered. The range of "Near Field Communication," the radio standard NFC, which enables contactless communication between the card and the terminal, is only a few centimetres. This means criminals must enter the victim's comfort zone very close. In addition, the signal strength can be attenuated by different materials.

AD-HOC INVESTIGATIONS

The BSI has re-enacted scenes from these videos to verify the reports mentioned and investigated whether contactless payments can be triggered unnoticed – especially when several NFC-capable cards are presented simultaneously.

For this purpose, various cards (checking account cards, credit cards, annual public transport season tickets and ID cards) that contain an NFC chip were brought into the reading field of a payment terminal in the most varied combinations. The results were neither clear nor fully comprehensible, however. In some cases, none of the cards were read, in others, one card was read but not the one closest to the reader. In further attempts with different cards, a specific card was always read out, regardless of its position in relation to the reader. There was definitely no consistent traceable interference from another or generally more cards that would have prevented a payment from being initiated.

In any case, this showed that debits cannot be triggered so easily in passing. This could not be reliably achieved with a wallet in the back pocket or a purse in a ladies' handbag, regardless of how many NFC-enabled cards were stored in the wallets.

SYSTEMATIC TESTS IN A DEFINED LABORATORY ENVIRONMENT

These preliminary investigations were further deepened in tests performed by an independent test laboratory. For the tests, different types of cards from a wide range of application areas such as credit cards, debit cards, prepaid cards, VDV cards and eID documents were used, as well as different readers such as payment terminals, mobile phones and specified reference devices.

In the case of readers or terminals developed on the basis of the EMVCo Contactless standard (cards with a payment function), no card should actually be selected when several cards are presented simultaneously. This is not the case for terminals based on ISO/IEC 14443 and NFC Forum. In this case, it is even intended that one card be selected from several cards.

This may explain how several cards acted differently in one reading field. For example, annual public transport tickets should still be recognised even if a credit card is transmitting in the same field. Several payment cards, however, should interfere with each other.

RESULTS

Tests carried out by the test laboratory also showed that EMVCo readers can select a payment card even if it is held in the reading field together with other payment cards. The anti-collision mechanism of the reader is therefore not always reliable.

SUMMARY

Studies involving different payment terminals have shown that the simultaneous presence of several contactless cards is no guarantee that unintentional reading of one of these cards will be reliably prevented. The only effective protective measure is the use of suitable protective sleeves in which contactless cards should be stored. This is the only way to ensure that unwanted communication between any reader and one or more contactless cards is prevented.

Fundamentally, however, the question arises as to how likely it is that attackers can locate the card in pant pockets or handbags without violating the victim's personal comfort zone. ■

Secure Electronic (Remote) Identification and Know Your Customer (KYC) Processes

Prerequisites and Common Rules for Europe to Combat Money Laundering and Financing of Terrorism

By Stephan Kohzer, Section Cyber-Security in the Public Health and Financial Services Sectors

In the spring of 2018, the European Commission formed a group of experts on the topics "Electronic Identification (eID) and Remote Know Your Customer (KYC) processes". The goal: Europe-wide Secure Electronic (Remote) Identification and harmonised Know Your Customer processes. On the way to a European Digital Single Market, cross-border frictions are to be reduced in these areas and common standards developed. The BSI is actively involved in this process – of course always with the aim of taking IT security into consideration with the solutions and standards that are discussed.

EARLY DETECTION OF UNUSUAL ACTIVITIES

With the overriding goal of combating economic crime, money laundering and the financing of terrorism, the EU member states have long since established state regulations. In Germany, the Money Laundering Act is particularly relevant in this respect. It sets comparatively high standards for the identification of customers of those subject to money laundering obligations – especially banks and insurance companies.

In addition to identification, other criteria must also regularly be checked and risk assessments carried out: What is the purpose of the business relationship? Do unusual cash flows take place? Are there links to so-called risk states?

Has the customer already become conspicuous or does he hold an office that is susceptible to illegal money flows? Clear identification, risk assessment and extended due diligence are part of the so-called “Know Your Customer (KYC) processes” and are intended to ensure that companies are familiar with their customers’ habits and that unusual activities are detected early on.

REMOTE IDENTIFICATION ON THE UPSWING

Everyone is familiar with identification by means of showing an identity card or passport when opening an account at a local bank branch. The physical identity card is checked for authenticity by trained personnel and a comparison is made with the applicant on site.

Over the course of time, other procedures have been developed that make on-site presence verification unnecessary. For example, online applications with identification at a post office (so-called PostIdent procedure in Germany) or, on a transitional basis, via VideoIdent/Videointerview, make it possible to identify customers who are not present. In contrast to PostIdent and VideoIdent, which are not completely digital and free of media discontinuity, online applications that use the online ID function/eID of the ID card are completely digital and free of media discontinuity. In order to establish the Digital Single Market in the EU, to strengthen competition and to use digital services regardless of nationality and residence, such procedures for remote identification will be indispensable in the future, preferably in their digital and media-break-free variants.

But, what happens if I, as a customer in another European member state, want to open an account online? How can I identify myself clearly from a distance? Which standards are necessary in order to be able to verify the electronic data sufficiently and assign it to the applicant free from any doubt? How can the various government, private and country-specific solutions be classified and compared with each other with regard to their security and trustworthiness?

The group of experts formed by the EU Commission discussed these exact questions and focused in particular on two main topics:

1. An inventory of the electronic procedures that are currently used in the various member states of the EU was conducted. At the same time, the question of how the customer data reached the providers was looked into. The security and trustworthiness of the collected data from the respective procedures were assessed.

2. Independent of existing procedures, a framework should be developed on the basis of the eIDAS identification and authentication means, which in the future serves as the basis for Europe-wide identification and usability/transferability of the KYC data collected. In particular, questions concerning the minimum data set, necessary and uniform trust levels, secure data sources and transmission paths, but also the standardisation of the data collected for the purpose of transferability were taken up here.

The EU Commission published the results of the two main topics in two separate reports at the end of March 2020.

HIGH REQUIREMENTS FOR EUROPEAN-WIDE SPECIFICATIONS AND STANDARDS

From the point of view of the BSI, the following points are of particular relevance for Europe-wide electronic identification and KYC processes:

With Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (in short: the eIDAS Regulation), an established standard that focuses on interoperability already exists. Future procedures – including those in the private sector – will be based on this standard.

It is also important that uniform guidelines and standards be consolidated within the EU. Otherwise, different solutions with non-comparable security levels would offer arbitrage opportunities. The increased use of the procedure with the lowest requirements would lead to alternative, more secure procedures being forced out of the market and the security level being fundamentally worsened.

The BSI will continue to follow the activities of the Commission and the member states in order to advance the goal of IT security in times of progressive digitalisation and on the way to a Digital Single Market and thus also provide technical IT support in the fight against economic crime, money laundering and the financing of terrorism.

More information:

https://ec.europa.eu/digital-single-market/en/news/reports-expert-group-eid-and-kyc-processes

United for a Secure Digital World

The vzbv and the BSI Cooperate to Advance Digital Consumer Protection in Germany

By Dr. Angelika Praus, Project Group Digital Consumer Protection

Cyber Security is a joint task. Effective consumer protection in the digital world can therefore only succeed within the framework of a cooperative approach. The Federation of German Consumer Organisations (vzbv) as an established player in consumer protection has a strong voice in the public eye and is an important partner of the BSI.

In a joint Memorandum of Understanding (MoU), vzbv and the BSI have committed themselves to a partnership-based cooperation for an initial period of three years. In order to protect consumers in the digital world, this cooperation will enable a combination of technical expertise, consumer law powers and effectiveness in the field. It is intended to create synergies that will directly benefit consumers.

In concrete terms, the partnership pursues these objectives:

- To promote secure networked IT systems and online services
- Information and education of consumers about the possibilities of reaction in case of damage
- Raising public awareness of options for protections in connection with digital applications
- Joint activities – if legally possible – to take preventive action against possible violations of the current legal framework in the area of consumer protection

This objective is intended to help industry increase the security of its products and applications and to create an appropriate level of resilience for consumers to threats and dangers to IT security.

THREE QUESTIONS TO KLAUS MÜLLER (EXECUTIVE DIRECTOR OF THE FEDERATION OF GERMAN CONSUMER ORGANISATIONS)

■ How can consumers be empowered in the digital world?
Digital products and systems are becoming more and more complex, making them difficult for many people to understand. Responsibility for IT security must therefore not be shifted onto consumers. For this reason, we are calling for secure and data protection-friendly technology design by manufacturers. From the very beginning, products and services must meet a high level of IT security according to the state-of-the-art – keyword: "Security by Design" – and be equipped with secure default settings – keyword: "Security by Default." Consumers must be able to rely on products and services meeting a high level of IT security already during their development and implementation and being provided with security updates during their lifetime. The data scandals of recent years show that clear legal regulations are necessary for this.

■ What added value does the cooperation between the vzbv and the BSI offer for consumers?
vzbv is increasingly dedicated to the topic of IT security. With the cooperation between vzbv and the BSI, we are

The Memorandum of Understanding between the vzbv and the BSI is available at:

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

„The aim of the cooperation is to create synergies that will directly benefit consumers.“

bundling our expertise and generating synergy effects. vzbv contributes its experience in law enforcement, political work and market observation. This ideally complements the BSI's outstanding technical expertise in the field of Cyber Security. Consumers will benefit from this.

■ **Which specific topics are particularly relevant to you in the area of digital consumer protection over the next three years?**

IT security is becoming more and more important with increase in networking. We need strong data protection. The protection of privacy has high priority. The rules of the game for the use of Artificial Intelligence are also becoming increasingly relevant for consumer protection. This is why vzbv is helping to shape them.

Brief Profile Klaus Müller

Klaus Müller, born 1971, has been a member of the Board of Management since May 2014
of the Federation of German Consumer Organisations (vzbv). The vzbv is the umbrella organization of 16 consumer centers and 26 other consumer policy-oriented associations. From 2006 to 2014 Klaus Mueller led the consumer center North Rhine-Westphalia. Previously, the economist was in politics active: From 2000 to 2005 he was Minister of the Environment in Schleswig-Holstein, until 2006 member of the Schleswig-Holstein state parliaments. From 1998 to 2000 Klaus Müller was a member of the German Bundestag.

Working at the BSI: Actively Shaping the New Normal

By Bettina Jäkel-Schmidtr, Section Human Resources Development

Already back in June 2020, the BSI started looking into the question of what positive experiences with the work done mainly in home offices can be applied to a future new normality. A project group has developed a model for this New Normal that is already being implemented in the ongoing corona crisis and will continue to be implemented after it ends. We all still remember the lockdown in March 2020, when sudden changes in our everyday working lives took place. The BSI also had to overcome many challenges: suddenly, most of the employees were mainly in their home offices, they met in digital meetings and the short informal channels for deciding on things in the coffee kitchen were no longer possible. This experience, which the Fraunhofer Institute for Industrial Engineering (IAO) describes as a "great achievement" and "community experience," was also experienced this way at the BSI. Everyone was proud, that the challenge could be mastered so well.

QUICK ADAPTATION TO THE NEW CONDITIONS

The BSI achieved a New Normality very quickly in the pandemic: a high rate of mobile working, the rapid switch to video conferencing and the digitalisation of skilled work, such as the switch to virtual job interviews, characterised this phase. The experiences with the changed work situation differed for each individual. Although many appreciated the home office as a more concentrated place to work, they also missed the chance to meet and talk to each other personally at work.

CHANGED LEADERSHIP

The BSI already started a process to further develop the management culture in 2019. The core of this process is the focus on an impact-oriented management style. The corona crisis and the discussion of a work culture in the New Normal have acted as a catalyst: As a result of the predominantly mobile nature of work, managers are challenged more than ever to define their leadership style through goals and results. Being present as a performance feature is no longer an option in the New Normal.

Since the beginning of the pandemic, managers have therefore been increasingly supported in their everyday management with a targeted canon of impact and employee-oriented leadership skills in (online) training formats.

A PICTURE FOR THE FUTURE

Already during the first few weeks under changed working conditions in the crisis, work began on documenting the experiences made as "lessons learned." Even before the general public discussion on the New Normal began, the management of the BSI commissioned the development of a vision of the New Normal. Its motto was: "Take positive aspects of the past months with you and suppress negative aspects."

An initial target picture of the New Normal was outlined in three online workshops with all departments, the committees and the equal opportunity commissioners participating. The process was completely digital, documented in a Wiki and was thus already part of the New Normal.

In the first workshop, the group analysed the actual change: What was the situation like before corona? How is it now? A total of 43 topics were identified in the four fields of action. In the second workshop, the change was described and initial guidelines for the target image were developed. Finally, the third workshop worked out which critical success factors and solution approaches still needed to be considered. The documentation of all workshop results in the internal Wiki created a collection, the so-called "treasure chest" that can be used for designing the New Normal even further.

DIFFERENT PERSPECTIVES FORM AN IMAGE

The format designed by HR Development and the cooperation within the group were already part of a new virtual normality. This working method in the workshops was highly efficient and brought many aspects and perspectives into the target picture. Only by taking this approach was it possible to develop a holistic view of the target image.

Following the workshops, the results were summarised in a two-page paper on the New Normal that was approved by the authorities. It describes the goals of a sustainable work culture at the BSI, which is to take the changed working and living environment during and after the corona pandemic permanently into ac-count.

It is still too early to grasp all the changes and their effects. For this reason, the BSI will continue to learn from the experience gained.

The mission statement will be taken into account in the future design and further development in all areas of the BSI. The implementation of the mission statement will create a sustainable framework for the future, not only to achieve the BSI's goals, but also to establish efficient cooperation across departments and hierarchies, and to promote employee satisfaction through a better balance between work, family and life.

With its New Normal image, the BSI is continuing on its path as a sustainable federal office, an attractive employer and a partner for the state, business world and society. For us, the New Normal is a catalyst for the digitalisation of the BSI. We want to be a pioneer for a modern authority with digital administrative processes. By working more digitally, we contribute to a sustainable society and the prudent use of resources (e.g. fewer business trips, commuting, paper consumption). ■

Guidelines in the "We" form were developed for the following four fields of action to describe the target state of the New Normal:

1. **Work organisation (How do we work?):** e.g. hybrid work; flexibilisation of place and time

2. **Work equipment (What do we work with?):** e.g. hard-ware and software adapted to the challenges; ergonomic equipment

3. **Leadership and cooperation (How do we lead?):** e.g. lead-ing and working at a distance; is more individual leader-ship necessary?

4. **Skills (What do we need to know and be able to do?):** e.g. digital skills; increasing communication skills; knowledge management

Order Your BSI Magazine!

Federal Office
for Information Security

Twice a year, the BSI Magazine "Security in focus" offers insight into national and international cyber security, digital society and IT security in practice. You can receive the latest issues by mail by subscribing to the distribution list with the form below.

I would like to subscribe to the following BSI publication:

□ BSI Magazine "Security in focus" (2/year, print)

□ The State of IT Security in Germany (1/year, print)

Last name, first name

....

Organisation

....

Street

....

Postal code, City

....

Email

....

Data protection consent:
I consent to my aforementioned personal data being used, electronically stored and processed by the BSI as the responsible body for the dispatch or transmission of the aforementioned publications. No data will be given to third parties without consent.

Date/Signature: ....

The Federal Office for Information Security, PO Box 200363, 53133 Bonn, Germany, is responsible for processing your aforementioned personal data. The information you provide will only be used to manage the sending or transmission of the information you have consented to above. You may revoke this consent at any time. Simply send an email to bsi-magazin@bsi.bund.de. Revoking consent does not affect the legality of prior processing before revocation. For more information on how we process your personal data and what rights you are entitled to, please refer to the "Data Protection Information" attached for ordering BSI publications.

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

....

Or you can register directly online: https://www.bsi.bund.de/EN/BSI-Magazine

....

If you no longer wish to receive BSI publications, simply send us an email at **bsi-magazin@bsi.bund.de.**

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 information: https://www.bsi.bund.de/datenschutzrechtliche-hinweise

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

IMPRINT

Published by:
Bundesamt für Sicherheit in der Informationstechnik (BSI)
53175 Bonn

Source:
Federal Office for Information Security (BSI)
Section B23 – Cyber Security for Citizens; Public Relations
Godesberger Allee 185–189
53175 Bonn
Phone: +49 (0) 228 999582-0
email: bsi-magazin@bsi.bund.de
Internet: www.bsi.bund.de

Last updated:
Dezember 2020

Content and editing:
Nora Basting und Mark Schulz, Federal Office for Information Security (BSI);
FAKTOR 3 AG

Concept and design:
FAKTOR 3 AG
Kattunbleiche 35
22041 Hamburg
www.faktor3.de

Printed by:
Appel und Klinger Druck & Medien GmbH
Bahnhofstraße 3
96277 Schneckenlohe
Internet: www.ak-druck-medien.de

Item number:
BSI-Mag 20/712-1e

Image credits:
Title: GettyImages © shapecharge; p. 4, BSI, GettyImages © Dong Wenjie; p. 10, FAKTOR 3 AG - Composing; p. 12, Screenshot-Composing BSI/FAKTOR 3 AG; p. 14, Bundesregierung Corona Warn App/FAKTOR 3 AG - Composing; p. 18, Shutterstock © Fit Ztudio; p. 21, © PopTika; p. 22, Shutterstock © Prokopeva Irina; p. 25, Hochschule des Bundes für Öffentliche Verwaltung; p. 26, BSI; p. 29, Thomas Popp © Matthias Rietschel; p. 30, GettyImages © Henrik Sorensen; p. 32, BSI, FAKTOR 3 AG - Composing; p. 36, BSI, FAKTOR 3 AG - Composing; p. 38-39, BSI; p. 40-41, BSI, Bundesministerium des Innern, für Bau und Heimat, Pexels © Errin Casano, Pexels © Pixabay, Pexels © worldspectrum, Pexels © alphatradezone, GettyImages © Dong Wenjie, Bundes-Verbraucherzentrale, Pexels © sarayut; p. 42, GettyImages © Kathleen Finlay; p. 43, GettyImages © Busakorn Pongparnit; p. 44, GettyImages © Artur Debat; p. 46, GettyImages © sorbetto; p. 49, Freepik © Stories; p. 52, GettyImages © Vectorios2016; p. 54, GettyImages © Westend61; p. 57, Gert Baumbach - vzbv.; p. 58, GettyImages © Hugo Donabella Mattos / EyeEm; p. 60, GettyImages © Gandee Vasan;

The BSI Magazine is published bi-annually. It is part of the Federal Office for Information Security's public relations work. It is provided free of charge and is not intended for sale.

Scan the QR code for the digital version of the BSI Magazine

https://www.bsi.bund.de/EN/BSI-Magazine

www.bsi.bund.de