

Security in focus

Digital Extortion with Ransomware

Cyber Security

Automotive Security:
From Production Right into
the Vehicle

BSI International

BSI and NATO:
Shaping Cloud Security in
the Alliance

Digital Society

Security Rather than Risk:
Digital Consumer Protection
in the BSI



Editorial

Dear readers,

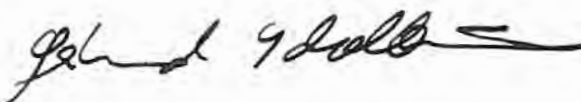
In news coverage, reports of cyber security incidents and cyber attacks on businesses and institutions have become a permanent feature. In addition to its diverse benefits, continuing progress in the digitalisation of our daily life and many business processes unfortunately also generates more attack surface for cyber criminals. That is why for state, economy and society, cyber security and robust security measures to protect against digital threats are more important than ever. What's more, the threat situation in cyberspace is tense, dynamic and multifaceted, so it has never been so high. This trend was confirmed in the BSI report published in October, "The State of IT Security in Germany 2022".

A key finding of the situation report is that blackmail with ransomware continues to be the main threat in cyber space. High-turnover companies, in particular, were the focus of attackers here. These attacks can use encrypted data to put pressure on the victims, and thus paralyse entire business processes. The administration of a district in Germany that was affected spent 207 days coping with the consequences of a ransomware attack. But, a typical consumer can also be a target of cyber extortion. This aspect is also confirmed by the Digital Barometer 2022, which was presented in November. A central pillar of our work in addition to detection and response is prevention. In the current edition of the BSI Magazine we want to sensitise you to the threat of ransomware. To do this, our experts have taken a closer look at different aspects of digital extortion.

But, as society, we are not at the mercy of this threat in cyberspace. In numerous projects, we have developed along with external partners approaches to solutions which illustrate this. In this edition, exciting insights can be found for example on the data security of consumers, cyber security in the automotive industry, the international work of the BSI in the NATO alliance, as well as the totally new offer for local governments – the BSI Road Show. As the federal government's cyber security agency, the BSI contributes every day in a holistic way to the digital security of Germany. After all, without information security, sustainable digitalisation would not even be possible.

I wish you enjoyable reading.

Yours faithfully



Dr. Gerhard Schabhüser,
Vice President of the Federal Office for Information Security



Table of Contents

06 – 07 News



Cyber Security

08 – 09 Automotive Security:
Cyber Security from Production
Right into the Vehicle

10 – 11 Cyber Security in Space

12 – 15 BSI Eavesdropping Counter-
measures at G7 Summit in Elmau
2022

16 – 17 The Cyber Security Network
– A Training Report

In Focus

20 – 21 Digital Extortion with
Ransomware

22 – 23 A Day at CERT-Bund

24 – 25 Protection is Possible in Every
Phase

26 – 27 What Cyber Crime and the
Industry Have in Common



The BSI

28 – 29 it-sa 2022 in Nuremberg

30 – 33 The State of IT Security in
Germany 2022

34 – 37 #Team BSI



IT Security in Practice

- 38 – 39 Heighten Cyber Security in Local Governments
- 40 – 41 The Perfect Couple: Information Security and Digital Administration
- 42 – 43 How Photos for Your Identity Card Will Be Transmitted to Authorities in Future
- 44 – 45 More Security in Road Traffic

BSI International

- 46 – 47 BSI and NATO: Shaping Cloud Security in the Alliance
- 48 – 49 Update for European Cyber Security

Digital Society

- 50 – 51 Security Rather than Risk
- 52 – 53 Helping Older People Live a Secure Everyday Digital Life
- 54 – 56 BSI Basic Tip: Nine Tips for a Secure Home Network

58 LEGAL NOTICE

Recognised: Cyber Security Label



BSI Vice President Dr. Gerhard Schabhüser and the CEO of the Cyber Security Agency Singapore (CSA), David Koh, sign bilateral agreement.

BSI AND SINGAPORE MUTUALLY RECOGNISE CYBER SECURITY LABEL

BSI Vice President Dr. Gerhard Schabhüser and the chief executive of the Cyber Security Agency Singapore (CSA), David Koh, signed at this year's Singapore International Cyber Week (SICW) a bilateral agreement for mutual recognition of the Cybersecurity Labelling Scheme (CLS) and the German IT Security Label.

In Singapore, products with the German IT Security Label of the BSI can now obtain a level 2 cyber security label. Labels from Singapore of level 2 or higher allow manufacturers to go through a simplified application process for the granting of the German IT Security Label. With the joint agreement with the CSA, the BSI continues to expand cooperation with international cyber security agencies. The joint agreement underscores the significance of the IT Security Label as blueprint for shaping European and international labels.

With the help of the IT Security Label, via short URL or QR code consumers can easily get information about the security features assured by manufacturers and providers for networked, internet-capable products and services.

Cyber Security² Video Series: Third Season Released

APP SECURITY – A CONVERSATION WITH EXPERTS

Apps are the companions of our everyday digital routine. Whether step counter, calendar or messenger – their use has penetrated deep into many areas of our lives.

But they can also pose a security risk. If at all, many security settings are only checked by apps during installation, and many users soon forget about them again soon after. But, when using apps, there are many settings which can help enhance security. In the seven episodes on the subject of app security, Michaela Hansert (BSI Division IT Security Consulting for State and Local Governments) and Martin Bregenzer (EU klicksafe initiative) talk about risks, the main security settings, data security and data protection, protecting devices and youth, and messenger apps.



Take a look now and safeguard app:



Playlist on YouTube:
<https://www.youtube.com/playlist?list=PLUE-Po9QcKRA5RXHrbWsZdv8xPXIWSwPCu>

The BSI on Executive Board of ENISA



Horst Samsel – Active for the BSI and ENISA

In June 2022 Horst Samsel, BSI Director-General Consulting for Federal, State and Local Governments, was chosen as representative for Germany on the executive board of the European Union Agency for Cybersecurity (ENISA). The BSI has represented Germany on the ENISA executive board for many years now, and is involved in numerous specialised working groups.

With the selection of Horst Samsel for the executive board the BSI can continue to support ENISA even more and specifically in the fulfilment of its mandated tasks. In this regard the intention is to work towards an agency that intensifies its role as multiplier for expertise on matters related to cyber security on the EU level, and serving as communication platform for cooperation between member states and other interested parties.

The current focus of ENISA work includes advancing certification schemes in accordance with the Cybersecurity Act (CSA) and providing support for operational cooperation in the EU. In the future, the focus will be on supporting the member states in the implementing of the second European directive to ensure a high level of network and information security (NIS2 Directive).

ENISA has received an ongoing mandate through the CSA since 2019. The overarching objective is to achieve a high level of cyber security in the entire European Union.

New Franco-German Common Situational Picture Published

Together with the French agency for information security, Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), the BSI has published a common situational picture. This fifth joint publication of the BSI and ANSSI deals with the subject of certification. It places special focus on the treaty concluded in the summer for mutual recognition of the BSZ (accelerated security certification) and CSPN (Certification de Sécurité de Premier Niveau) certifications.



New Brochures on Cyber Security and ePayment Solutions

The brochure “Cyber-Sicherheit für KMU” provides small and medium-sized enterprises with an easy introduction to improving the level of cyber security. With the help of 14 questions the main aspects are highlighted and practical tips provided. The new publication “ePayment – Schlüsselfaktor der Digitalisierung” (ePayment – Key Digitalisation Factor) provides a checklist for agencies that intend to introduce online payment procedures. Essential information that is important for electronic payment methods in agencies is also explained.

All BSI publications can be found here:



BSI Publications:
https://www.bsi.bund.de/EN/Service-Navi/Publikationen/publikationen_node.html

Automotive Security: Cyber Security from Production Right into the Vehicle

By Marco Krambrich, Division National IT Situation Centre, Analysis and Forecasts

The effects of the Corona pandemic continue to be felt everywhere in the automotive industry, but mostly in the area of supplier parts, products or services. The situation is primarily impacted at the moment, however, by Russia's war of aggression against Ukraine, and the associated economic and increasingly cyber security-relevant effects on the German automotive industry. The situation as it stands.

The quality of cyber attacks is becoming ever more sophisticated and targeted. In the view of the BSI, ransomware attacks remain the largest operative threat to cyber security – particularly for the IT systems of automobile manufacturers and suppliers. Recently, for example, a German supplier of car parts had to deal with substantial production outages in many plants due to ransomware. Only a month later could production for the most part be returned to normal operations.

To make matters worse, the Russian war of aggression against Ukraine is being increasingly accompanied by actions in cyberspace, which are also affecting the German automotive industry and endangering cyber security. Included here are DDoS attacks aiming to paralyse entire web sites, and the intensive activities of so-called hacktivists.

In the recently released second edition of the industry situation overview "Automotive 2021/2022", the BSI presents an industry-specific overview of the state of cyber security in this area and provides information on incidents and vulnerabilities.

Further information:

Automotive industry situation overview:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchenlagebild-automotive-2021_2022.html?nn=520690



CYBER SECURITY IN THE VEHICLE AND IN DIGITAL PRODUCTS

Both electromobility as well as digitalisation remain topics of high relevance for the automotive industry. Here, the cyber security of vehicle systems is a feature that is key to the successful implementation of digitalisation. Newly introduced controls oblige manufacturers to take cyber security into account in product development, and design cyber security management systems that quickly allow suitable countermeasures should new vulnerabilities be exposed.

Various research undertakings have highlighted how susceptible to cyber attacks vehicle systems are that are equipped with radio communication or are linked with background systems. This includes:

- the failure of infotainment systems due to faulty metadata,
- opening vehicles through insecure API tokens,
- replay attacks on locking systems,
- the interruption of fast-charging operations.

CONNECTED DRIVING

The development of automated and autonomous driving continues to make great strides. This is because increasing amounts of computing power and larger quantities of data are available to develop methods and systems with artificial intelligence (AI). Aside from the new functionality and increased performance it generates, however, the use of AI in automated and autonomous driving also creates new challenges.



CYBER SECURITY IN PRODUCTION PLANTS AND PROCESSES

In the area of production the extent of IT connectivity and automation becomes particularly evident: On modern production lines a large number of components are interconnected – in everything from sensors to production robots. With the increase in IT connectivity, the attack surface also increases, because these systems can also be linked to the corporate network or service provider and partner/supplier networks, and are to be accessible to some extent over the Internet.

On top of the risk in general from ransomware attacks, examples of malware are repeatedly being seen that are particularly focused on industrial control systems (ICS). The purpose of these are to collect information or perform manipulations.

Automobile manufacturers bear an active responsibility for protecting their own IT systems and networks, and for this they require a suitable vulnerability management system. Anyone without such a system is at enormous risk, because production outages caused by cyber attacks can quickly threaten a business' viability. As conveyed by the theme of this year's 18th IT Security Congress, cyber security has to be a top-level priority and organised with adequate resources as permanent feature of a company's risk management efforts.

Even improving the software quality makes an important contribution to increased cyber security. A particular challenge in this regard are the complex software supply chains, which can make it more difficult to locate and rectify vulnerabilities. That is why the BSI calls for targeted implementation of measures for better software quality in IT products. To this end the BSI actively encourages such concepts as a Software Bill of Materials (SBOM)¹ and the Common Security Advisory Framework (CSAF)², to optimise Coordinated Vulnerability Disclosure processes (CVD processes). CVD processes are used to handle messages about vulnerabilities in IT products and allow security analysts who

have discovered vulnerabilities in IT products to report them to a central address and assist in their rectification and the corresponding release of patches.

BSI MEASURES AND ACTIVITIES

To shape security in the area of digitalisation, which is so important for Germany as location for business and automobiles, and to establish a reliable framework for investment and innovation the BSI and the Federal Motor Transport Authority (KBA) work together closely on questions related to cyber security. For example, with new rules for the approval of vehicles, the subject of cyber security is to be firmly established throughout the entire life cycle of a vehicle, to be able to better prevent risks. The exchange of information with the automobile industry necessary for the actual putting into actual application is proactively promoted by the BSI and the German Association of the Automotive Industry (VDA).

For more security in new technologies such as artificial intelligence, 5G or smart home/smart factory, the BSI devises among others practical security requirements, standards and recommendations for action.

In future, new rules for entities of special public interest (UBIs) are to help achieve a more broad understanding of the cyber security of these entities by having them communicate to the BSI information about relevant certifications, audits, IT disruptions or other measures.

Implementing these tasks in a holistic way in the automotive area is a complex and multifaceted challenge. It remains incumbent on the industry through suitable development processes to guarantee cyber security company-wide and throughout all phases. ■

¹ In an SBOM all the components and dependencies of certain software are listed to allow efficient checking of whether a product is affected by a known vulnerability. ² A machine-processed format for security advisories.

Cyber Security in Space

By Dr. Johanna Niecknig, Division Air and Space IT Security Systems

“Dependent on Space” – this is the title of an article in edition 2021/01 of BSI Magazine that discusses the growing significance and threat landscape for satellite systems. The article also provides some initial answers as to how the BSI views this subject and the measures the federal cyber security agency takes to meet the new challenges and to strengthen the cyber security of infrastructures in space.

WWithout satellites, our day-to-day lives would not be the same; Navigating with GPS would be impossible, television and Internet quality would be poorer and increasingly less, and weather forecasts would be less detailed and dependable.

We only become aware of how satellites influence our lives when their services are gone – i.e. when security objectives such as integrity and authenticity and sometimes the confidentiality of the signals and data cannot be assured.

Critical infrastructures (KRITIS) depend much more on applications requiring satellite support than society in general. They are used to perform tasks such as monitoring rail or air traffic, synchronising communication and electricity networks, and reliable financial transactions. At the same time, they play a key role in observations and exploration of the earth, such as researching climate change, or coordinating emergency and rescue services for disaster management. But, the importance of satellites is growing in all areas also in digital communications.

As federal cyber security agency, the BSI is responsible for strengthening the cyber security of such systems and ensuring the availability of services through integral and authentic communication. For this the BSI has systematically identified strategic fields of action and specific goals for implementation, and derived various measures to be implemented in coming years.

OVERVIEW OF THE PLANNED MEASURES

As of 2023, BSI will appoint a specialised Division for information security in space infrastructures. It will act as central, coordinating office for cyber security for civil as well as military air and space applications and systems, and shall take the following measures:

- Identification of minimum requirements for cyber security in space
- Development and updating of specifications and recommendations as well as provision of development advice already in early project phases
- Advice and services related to cyber security in the areas of minimum requirements and approval
- Active participation in or holding of events as well as publication of articles technically related to aerospace systems
- Standardisation of the minimum requirements in collaboration with international partners

Initial measures have already been implemented. In 2022 the BSI, the companies OHB and Airbus as well as the German Space Agency at the German Aerospace Center (DLR) jointly developed recommendations for minimum protection requirements for satellite missions. These have been made available to interested users (manufacturers, operators and suppliers of satellite systems and components) in the form of an IT-Grundschutz profile for space infrastructures.

Strategic Fields of Action of the BSI for Shaping Cyber Security for Space Infrastructures



Secure and self-determined action in a digitalised environment

Powerful and sustainable state-wide cyber security infrastructure

State and economy share common cyber security mission

Active positioning of Germany in European and international cyber security policies

RECOMMENDATIONS FOR MINIMUM PROTECTION REQUIREMENTS FOR SATELLITE MISSIONS.

The IT-Grundschutz profile contains on one hand requirements based on the components defined in the IT-Grundschutz Compendium. It supplements specific requirements, however, that are not listed in the IT-Grundschutz and which apply to the different aspects of the respective life phases of satellites (design and development, test, transport, start campaign, in-orbit phase, operation, and decommissioning). Insofar, as it is relevant for the realisation of the different phases, the IT-Grundschutz profile also addresses the corresponding Divisions of the ground segment. In order to formulate recommendations for a uniform minimum protection level for all currently conceivable satellite missions, the IT-Grundschutz profile must be based on a suitable protection requirement category (Normal). Only in this way, the scope of the identified requirements encompasses all launched satellites in orbit.

The IT-Grundschutz profile recommends, for example to apply the Crypto Concept (CON.1) module to control every satellite, to enable adequate protection of confidentiality, integrity, and authenticity of the data and connections. This module should be individually adapted, dependent on the mission and its criticality, such as through the selection of suitable cryptography methods. The BSI will report on the implementation of the further measures, and is available at any time as technical expert for cyber security in space. ■

IT-Grundschutz profile

The IT-Grundschutz profile serves as model security concept intended to help facilitate the implementation of IT-Grundschutz for institutions in the aerospace industry.

Further information:



Cyber security for space infrastructure:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.pdf?__blob=publicationFile&v=2



IT-Grundschutz profile for space infrastructure:
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_Space-Infrastructures.html

BSI Eavesdropping Countermeasures at G7 Summit in Elmau 2022

By Dr. Astrid Schumacher, Head of Section IT Security Consulting and Security of Classified Material, and Uwe Beckert, Head of Division Counter-eavesdropping

In the framework of Germany's G7 presidency, in June of this year for the second time the meeting of the heads of state and government of the seven leading industrialised nations in the world took place, the G7 summit at Schloss Elmau in Bavaria. Essential for an atmosphere of trust at this meeting was that the conversations remain confidential and the content of the discussions would not find its way into the public sphere or the hands of unauthorised third parties. Ensuring the confidentiality of these conversations in Elmau was the task of the counter-eavesdropping experts at the BSI.





Schloss Elmau

Preparations for this began at the BSI already many weeks before the summit – with consultations between the BSI and the Federal Foreign Office (AA), which was formally the host of the summit. This included questions related to the necessary technical and organisational measures for ensuring confidentiality. Also clarified here was which parts of the event were to be deemed as particularly in need of protection. The results of these consultations flowed as “hierarchy of the rooms” into a so-called “room book” which ultimately served as reference and working basis for everyone involved.



Use of testing tools on location



Use of a direction-finding vehicle



Behind the scenes: interpreter facilities



Installations in conference table

WHERE ATTACKS CAN OCCUR

At international events it is common practice to install interpreter facilities in order to synchronously translate the discussions into the different languages of the participants. Problematic from a security point of view are facilities which transmit the content of discussions via invisible infra-red light. For example, infra-red radiation can penetrate windows virtually unhindered. This can lead to the conversations being eavesdropped outside with relatively little effort, even from far away. That is why the BSI advocated for the exclusive use of wired interpreter technology at the G7 summit.

Another vulnerability can be private mobile devices such as smartphones, tablets or smartwatches, which participants bring along to confidential discussions. If it cannot be ruled out with certainty that malware on such devices is recording the content of conversations and sending it to unauthorised parties, an enormous threat to the confidentiality of the discussions exists.

For this the BSI offered the G7 the use of a mobile communication detection system, with which it is possible not only to detect devices that were brought in without authorisation, but also to locate them. In addition to that, for the event itself, on the recommendation of the BSI a ban on mobile communications was issued – and enforced – for confidential meetings. Also worth mentioning in this context is the potential use of

IMSI catchers during the event. To prevent this problem, IMSI catcher detectors that can detect this threat were put to use throughout the entire event.

BSI COUNTER-EAVESDROPPING ON LOCATION

The work of the counter-eavesdropping team during the G7 summit consisted essentially of two tasks: checking rooms that were at risk for hidden monitoring devices and the continuous search for anomalies in the high-frequency spectrum used for wireless communication, which would indicate monitoring devices.

The room checks were carried out in the conference rooms and areas which were intended for confidential bilateral discussions. They began in the conference furnishings with the sealing of hollow spaces, which could serve as hiding place for eavesdropping technology. In addition to the visual inspections, the rooms and all the technical infrastructure such as lighting and wiring were also inspected using special counter-eavesdropping testing devices.

At the time the rooms were furnished, high-frequency receivers and antennas were installed. Ideally, this is done as close as possible to conference activities, to expedite the detection of suspicious signals. For that reason the meeting tables in Elmau were set up with a large hollow space at the foot, which had room for the technology. The receivers were controlled over a



G7 summit at Schloss Elmau

The team from BSI counter-eavesdropping

sufficiently high-speed IP network which the existing network infrastructure could use. From a central location near the interpreter management area and interpreter booths the technology could be controlled and the measured results analysed.

Additionally, a BSI measurement vehicle was parked on the grounds of the conference facilities, also in the direct vicinity of the meeting rooms. The BSI also installed high-frequency receivers and a powerful direction-finder system there. With this it was possible beforehand and during the discussions to compare unusual high-frequency signals that could indicate an illegal monitoring attempt with the measurements from the conference rooms, and make an assessment as to whether the source of the signals was inside the conference building or outside.

SUMMARY: NO EAVESDROPPING TOOK PLACE AT ELMAU

The counter-eavesdropping work of the BSI, which, by the way proceeded without drawing any undue attention, came to an end with the conclusion of the G7 summit, without our

employees detecting any illegal eavesdropping attacks. Even the monitoring of the mobile communications turned up nothing conspicuous, so the entire summit was held without incident. Through the considerable efforts of the BSI, the confidentiality of the discussions could be guaranteed at all times. Likewise, the IMSI catcher detector and the WLAN and Bluetooth monitoring revealed no conspicuous signs of IMSI, WLAN or Bluetooth catcher use.

With these results, the counter-eavesdropping of the BSI once again demonstrated that, even with this kind of sensitive political event, it is possible to protect words spoken in confidentiality against eavesdropping by unauthorised listeners. ■

The Cyber Security Network – A Training Report

The Cyber Security Network (CSN) Is a Voluntary Association of Qualified Experts that Offer Their Expertise and Know-how for the Purpose of Rectifying IT Security Incidents.

By Angelika Jaschob, Division Cooperation with Manufactureres and Service Providers

The CSN makes available a digital training kit with free training and game collection. With this material, incident management can be trained in a playful way.



Ransomware training unit



Different role game cards for practice

“The intention is to provide both companies as well as helpers an opportunity to practise mastering IT security incidents in a secure environment”, remarks Matthias Mehrtens, Professor for Cyber Security Management at Niederrhein University.

What’s it like in a regional forum where emergency situations are trained?

IT SECURITY CAN BE TAUGHT

“It is Tuesday afternoon, 5 pm. Six digital first-aid helpers, a start-up entrepreneur and an incident expert of the Cyber Security Network (CSN) meet in Bonn-Rhein-Sieg University of Applied Sciences at a regional forum – just as they do every first Tuesday of the month. Here, they talk about the latest IT security incidents and new forms of attack, and exchange stories relating their experiences in handling incidents. Today, there is a special item on the agenda. The forum leader has downloaded the ransomware role game from the training kit of the CSN and prepared it with the help of the instructions. The aim is to practise dealing with a situation involving digital extortion, but in a secure environment.



Training kit role game



Training unit: The CSN's digital rescue chain

Usually it is common to do a “Tour de Table” at the start of a forum meeting, during which each participant contributes actual experiences or questions. But, today everyone is looking forward to the training unit, so that this exchange of experiences.

The afternoon is centred around the (fictional) retirement home “House Weinstock”, with 30 employees and 75 residents. On the weekend an encryption trojan infected and encrypted the IT systems of the home and completely knocked out the network. To decrypt the system, the attackers are demanding a large ransom payment.

The forum leader introduces the role game as moderator. Each participant can select one of eight role game cards, and then learn their particular role. Aside from the role of an incident manager, there is a role of a managing director who has no affinity to IT subjects, a role of a young IT manager who in fact is currently on vacation, and a role of a staff member of the IT service provider.

The fact that medications for the home residents cannot be properly provided without the data on the tablets of the home staff makes the IT breakdown in the retirement home so precarious. Not only that this situation makes it impossible to administer medications, some of which are critical, it also quickly upsets concerned relatives. On top of that, a local newspaper has heard of the incident and a rightly inquisitive journalist is on the doorstep. Finally, also the police have been notified and are attempting to investigate the details of the case.

The next hours pass with everyone playing their role and discovering where they are helpless to act. Hectic discussions take place, but they also talk shop about potential further steps. Happily, an incident expert is also on hand, asking the right questions and analysing the situation objectively, which qualifies him to act as crisis manager.

In the training centre of Bonn-Rhein-Sieg University it was thus possible to solve the IT security incident after only 60 minutes: The retirement home was able to generate a substitute system from an old backup, and thanks to the professional crisis management, the overall situation could be quickly de-escalated.

Following the role game a debriefing takes place where the forum leader offers her impressions as neutral observer and summarises what happened. She also presents some recommendations from the BSI on the topic of ransomware. Afterwards, the group spends some time discussing how they felt in their roles. Finally, everyone agrees they want to play out further training units in the forum setting. “I wouldn’t have known how to react in such a situation,” says one of the participants. “But one thing I do know now is that I feel more optimistic about the future after going through the training unit, because I won’t be so unprepared should I ever really be confronted with such a ransomware incident and its consequences.”

FROM TRAINING TO REALITY

The fact that such scenarios are not just found in the realm of theory was demonstrated by an IT security incident in June of this year in which an incident expert of CSN assisted a medium-sized energy company that had been attacked and partially knocked out by a ransomware attack. Thanks to an emergency plan, the consequences ended up being relatively mild.

For attacks, the CSN has developed a “digital rescue chain”, which specifies who is responsible for which task at what point of the process. The rescue chain includes everything from support through checklists, to telephone support by the CSN, right to a team of incident experts who can work on location. Thus the CSN brings together qualified helpers who can act in a coordinated way in case of an incident.

HOW WELL IS YOUR COMPANY PREPARED FOR AN IT SECURITY INCIDENT?

If you want to know how well your company is prepared for an IT security incident, you may find out with a self-evaluation test from the CSN.

With this roughly five minute test, small and medium-sized enterprises – but private individuals, too – can test their ability to react to IT security incidents. The test covers five questions about IT infrastructure and IT processes. Additionally, it includes questions related to responsibilities of staff and how passwords are handled in the company. The test also refers to documents and detailed instructions that can be used as aid for improving your own cyber resilience. ■

Take advantage of the free offer and participate in the Cyber Security Network.

Further information:



Cyber Security Network:
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

E-mail: info@cyber-sicherheitsnetzwerk.de



In Focus

Digital Extortion with Ransomware

Digital Extortion with Ransomware

Attacks with Major Damage

By Korbinian Barthuber, Division Incident Response and Liaison Office to the National Cyber Response Centre

Ransomware refers to malware that restricts or prevents access to data and systems, particularly through the use of data encryption. Release of the resources is only given in return for a ransom payment. According to the current BSI report “The State of IT Security in Germany”, attacks with ransomware are one of the biggest cyber threats faced by state, economy and society.

Ransomware attacks involve attacks on the security objective of availability, and are a form of digital extortion. Attackers exploit errors such as improper use, badly configured systems, obsolete software, or inadequate data security. The payment of the ransom money is usually demanded in electronic currencies (usually bitcoin or monero).

Ransomware is effective because of its directly noticeable effects. In contrast to classic malware such as banking trojans, botnets or phishing mails, the damage takes effect immediately and has tangible consequences for the victim. Here, no credit institute reimburses the damage (banking trojan) and the PC does not just work slower (botnet), but often not at all. In the case of a ransomware attack, for example, all saved files can be lost, important company data can become inaccessible, or critical services unavailable.

The best protection to reduce the consequences of such attacks are preventive measures such as offline backups, which are isolated from the IT systems.

RANSOM PAYMENT OR DATA RESTORATION?

Since the psychological stress of affected victims after a ransomware attack is so bad, the ransom is often paid in the hope of quickly regaining the ability to work again. Apart from the fact

that there is no guarantee that the data will be released, depending on the quality of the decryption tool the black-mailer provides, it may also be possible that the restoration of a system using specially stored backups would be quicker.

Aside from the encryption of data, cyber criminals also often threaten to make the stolen data public, to put even more pressure on the victim. Potential victims include institutions of all sizes – ranging from micro-businesses to authorities and companies providing critical infrastructure, up to large international corporations.

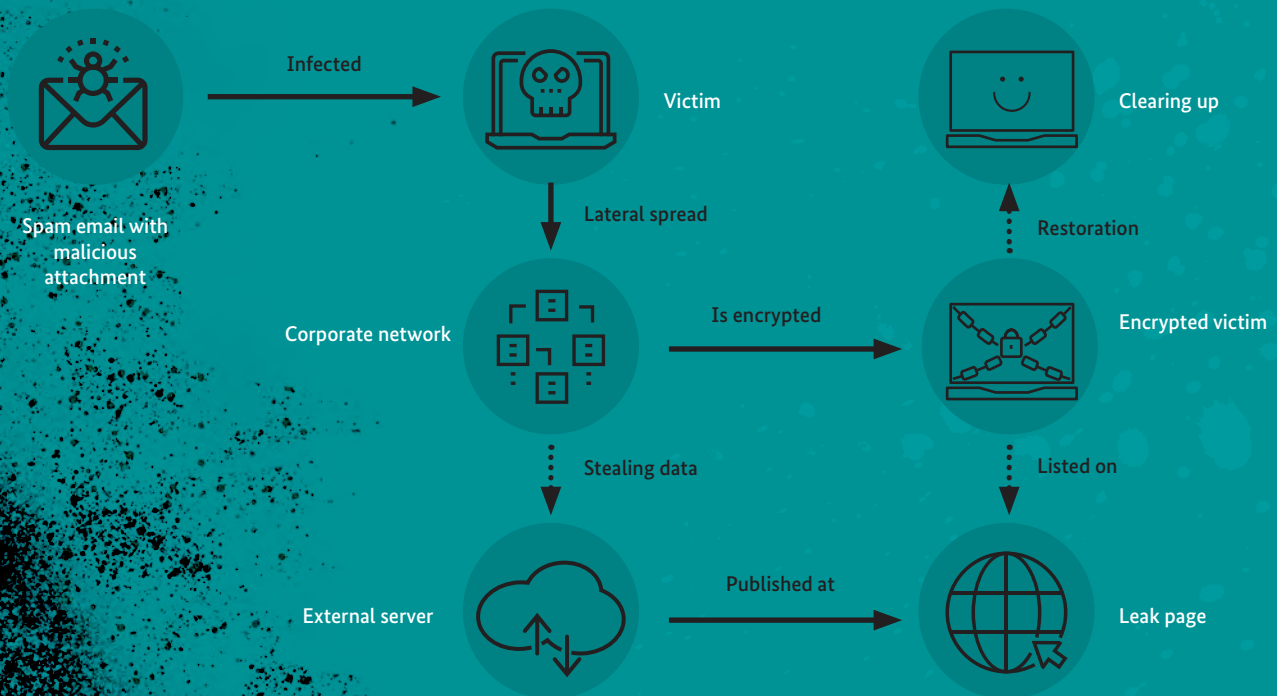
Not every ransomware attack can be prevented, because new ransomware can also make use of new paths of attack. In most cases, however, it is definitely possible to prevent successful attacks against enterprises, authorities and IT service providers. With preventive measures it is also possible to get the effects under control more effectively.

TYPICAL SEQUENCE OF A RANSOMWARE ATTACK

The most common target of attack is the human being. On client systems a primary point of attack is e-mails with a harmful attachment. In corporate networks, open or vulnerable or badly secured and externally accessible servers open the door to attackers.



Simplified portrayal of a ransomware attack



Cases of malicious attachments often involve Office files with VBA macros, .iso and .lnk files, or (encrypted) zip files with password directly supplied. In the case of servers, vulnerabilities are often exploited. In the past this has been, for example, CVE-2019-19781 (“Shitrix”) for Citrix ADC and Gateway or CVE-2021-34472 (“ProxyShell”) for Microsoft Exchange.

Aside from that, also remote access without two-factor authentication can represent risks. With servers, in particular, the actual attack might begin months after infection. Such initial penetration is often traded as access-as-a-service and sold to other attacker groups.

After gaining the access, attackers usually subsequently load more malware to elevate privileges and (semi-)automatically take over the network of the victim – right into the central components of privilege administration (Active Directory). Once this happens, the corporate network is completely compromised and cannot be trusted anymore.

Now the attackers possess all privileges, for example to create user accounts with administrator privilege, to view data, or to set up back doors. Data is stolen (“data exfiltration”) to threaten with their publication should the victim not be prepared to pay a ransom (“double extortion”).

Ultimately data is encrypted on as many systems as possible, and backup systems in particular, usually without impairing the operating system itself. Instead, the attackers leave messages with instructions on how the victim can make contact to negotiate.

The victims themselves are faced with the challenge of restoring their systems and data. Depending on the extent of the impact, interim operations must be organised and the incident communicated to stakeholders such as owners, customers and partners. ■

A Day at CERT-Bund

– and What Happens When a Ransomware Incident Is Reported

By Veselina Hensel, Division Mobile Incident Response Team (MIRT), and Letitia Kernschmidt, Division Incident Response and Liaison Office to the National Cyber Response Centre

Around the clock, reports are sent to the national IT Situation Centre which are received, evaluated and – depending on criticality – escalated by the “Computer Emergency Response Team” (CERT-Bund). Within in the legal framework, affected parties can receive support in the form of telephone consultations, the provision of helpful documents, the performance of technical analyses, or even on-site assistance.

A Thursday in the year 2022, ...

13:47

A report from an agency is received in the national IT Situation Centre stating the agency was hit by ransomware and is requesting assistance. In line with the process, the report is forwarded to CERT-Bund.

15:00

In a video conference the affected agency reports that the situation on-site is tense and the extent of the damage unclear. Essential control technology has broken down completely, so that operations can only be kept up for a short time with great effort. Preventively, all other central services were shut down. An offence has already been reported.

13:52

Initially, the duty officer conducts a phone call with the victim, during which it quickly becomes clear that the incident is serious. Since the victim is a federal agency, the BSI can offer extensive support in accordance with its legal mandate. From this point onwards an incident manager takes responsibility for the case.

16:00

Based on the descriptions, the BSI offers to support the agency on-site this very day. The agency accepts the offer. Since the control technology is also affected, the team with expertise in industrial control systems (ICS) is requested to participate. The time before departure is used to complete organisational activities, such as checking and loading the required equipment.

07 15

All team members are on the way to the affected agency, which in the meantime has succeeded in isolating samples of the malware and sending them to the BSI. While they are under way, the samples are forwarded to a colleague from the malware analysis team.

20 30

On arrival of the BSI team, everyone involved meets for an initial discussion. Here, it is essential to establish a common understanding, to define the objectives of the support mission, and to clarify any open questions. Based on this, further steps are planned, responsibilities defined, and tasks assigned. The aim is to bring order into an emergency situation, which affected parties are usually not sufficiently prepared for.

At the same time, all relevant systems and data (e.g. log data) are forensically secured. Since the virtual machines for the building automation and control systems are encrypted for the most part, following a technical discussion it is decided that the BSI may take away the two hosts for further analysis. Additionally, an initial analysis of the malware and rules for detection are now available, which are handed over to the affected agency.

22 30

The incident manager finalises an end-of-day report and sends it to a predefined distribution list. For now, that wraps up the work on-site!
In the national IT Situation Centre the findings of the team on-site are processed further overnight and prepared for the situation products of the BSI.

The next day

03 30

At the BSI the initial findings from the incident are prepared anonymised for a warning notice and published later via e-mail, the BSI website and the CERT-Bund Twitter channel. On-site the analysis and support work begin again.

11 20

The incident has now also been picked up by the media, which means that the press office must process initial enquiries. Further enquiries from the national and international partners as well as agencies in the National Cyber Response Centre need to be coordinated and replied to. In the course of the daily situation review the incident is presented and discussed internally at the BSI.

13 00

The BSI's own threat intelligence team fills in the findings with further details and shares them anonymised with target groups of the BSI via the Malware Information Sharing Portal (MISP). The Bundes Security Operations Center (BSOC) in the BSI also utilises this information to detect any attacks on federal networks.
The incident, including all further findings of the BSI, is recorded anonymised in the daily situation report of the BSI and shared with the target groups of the BSI.

16 00

Initial analysis results and defined measures are discussed. Based on this, the affected agency must plan and implement the eradication and recovery of operation over the coming days and weeks.

... and what now?

Depending on the case, further support can continue on over several weeks or even months. For this there is no one-size-fits-all approach, because each case is unique and so requires a different or possibly new and to some extent even creative approach. The only constant in life is change, so they say, and a job at CERT-Bund is also subject to constant variation. But this is exactly what makes it so varied and interesting!

Protection is Possible in Every Phase

From Backup to Contingency Plan: Identifying and Implementing Response Measures

By Maximilian Winkler, Head of Division Mobile Incident Response Team (MIRT)

A ransomware attack consists of multiple steps. For each phase of such an attack countermeasures exist preventing further exploitation as well as limiting potential damage. In this article we present a selection of these measures.

Among the biggest threats to IT infrastructures is the encryption of data via ransomware. This is most evident when the encryption of IT systems threatens the economic survival of a company or rendering public authorities incapable of performing their responsibilities.

However, encryption is in fact merely the final step an attacker takes after previously spending much time in a compromised network. For each phase of a ransomware attack, countermeasures exist that can successfully prevent attacks or at least limit their effects.

Attack phase 1 – intrusion

The three most common attack vectors of ransomware groups are phishing, the exploitation of vulnerabilities, and access through poorly secured external access points. Effective measures exist for each of these attack vectors.

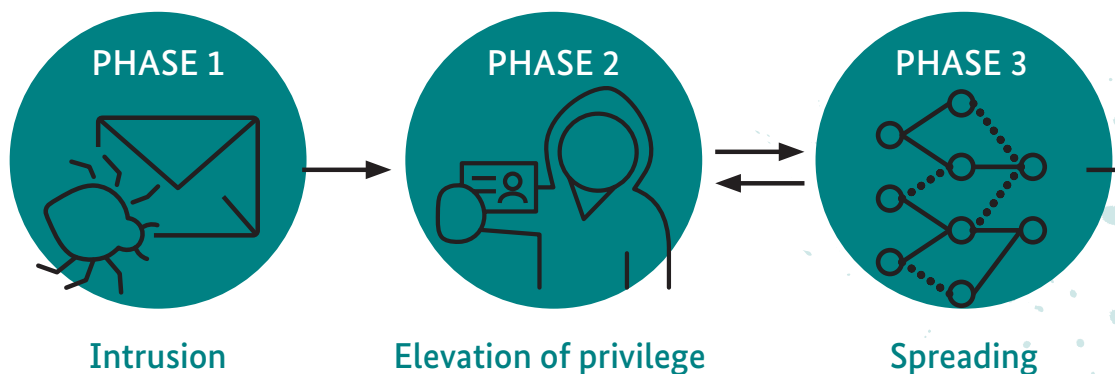
Phishing countermeasure: e-mails and sensitisation

The BSI recommends e-mails that are encoded as “text only” or “pure text”. In contrast to coding as “HTML e-mail” they cannot contain any macros or hidden commands. It is also impossible to hide any web addresses. For example, in an HTML-coded e-mail a link with the name “www.bsi.de” could in actual fact

point to a malicious web page. If text-only coding is impossible or undesirable, at least the execution of active content in HTML e-mails should be suppressed, so that malicious scripts cannot be executed anymore.

In the course of sensitisation measures, employees should be provided with practical training on risks when working with e-mails. This especially applies to employees from company areas (such as the HR or marketing departments), who have to deal with high volumes of e-mail communication from external sources.

Simplified portrayal of a ransomware attack



Vulnerability countermeasure: patches and updates

In order to prevent infections based on exploitation of vulnerabilities that have already been fixed, applied without delay – ideally via over a centralised software distribution system. Patches fixing critical vulnerabilities as well as patches for exposed applications like firewalls or internet facing web servers should be given priority.

Remote access countermeasure: multi-factor authentication

Cyber criminals often attempt to install ransomware on systems through compromised remote access points. That is why external access should also be protected by VPN in combination with multi-factor authentication.

Attack phase 2 – elevation of privilege Countermeasure: secure administrator accounts

Privileged accounts should generally only be used for administrative activities. In particular, such accounts should never be used for reading e-mails or surfing the Internet. For such “normal” activities, administrators should also create a “normal” user account. Privileged accounts should always be protected by multi-factor authentication. Domain administrator accounts should never be used for the administration of client systems.

Attack phase 3 – Lateral Movement Countermeasure: network segmentation

Strict network segmentation helps limit damage, because the infiltration of ransomware can only reach systems in the compromised segment. Safe use of administrator accounts is necessary for this too (refer to previous measure), because otherwise a central component of the security concept is undermined.

Attack phases 4 and 5 – encryption with/without prior data exfiltration

Countermeasure: backups and data storage

Backups are the best protection against the effects of encryption caused by ransomware, because they ensure direct availability of data even if encryption occurs. For this, however, the data must be saved on an offline medium, which is disconnected from the network backup process. Beside the backup, the planning and preparation of restoring systems from the backup as well as training this process regularly is required to ensure that complications related to restauration are detected before an actual incident.

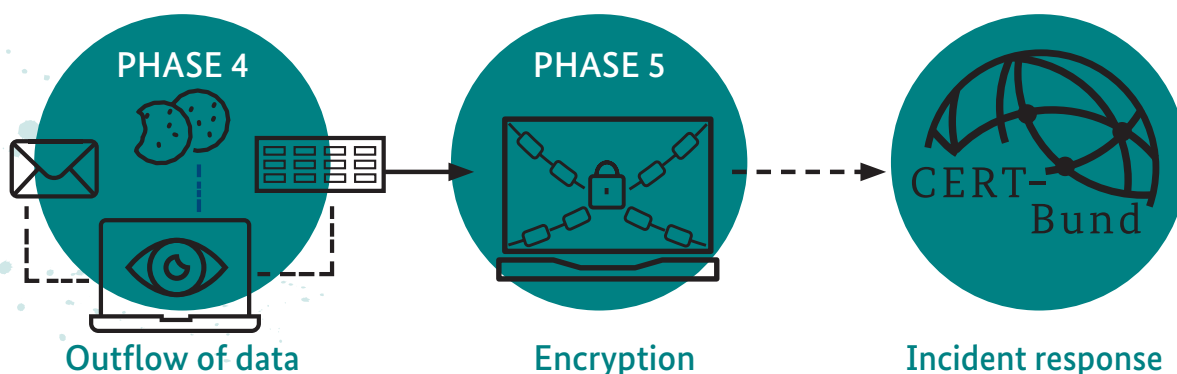
Measure: contingency plan

A contingency plan for emergency operation and remediation should exist for the worst-case scenario of a successful attack involving the encryption of all systems in a network. The processes for reacting and restoring mission-critical systems should be trained at regular intervals. In particular, mission-critical systems should be identified in advance and alternative communication options prepared outside of the compromised network. Important telephone numbers of contacts should be kept offline as hard copy.

Further information:



Ransomware information portal of the BSI:
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html



What Cyber Crime and the Industry Have in Common

Division of Labour, Outsourcing and Profit

By Alexander Härtel, Division National IT Situation Centre, Analysis and Forecasts

A closer look at practices of cyber criminals that blackmail companies with ransomware for financial reasons reveals surprising parallels to the real industry.

In the IT branch as well as in traditional areas of the industry different services are outsourced. In the IT branch there is software-as-a-service, for example, but the operation of infrastructure or the processing of data can also be outsourced.

Outsourced services such as this are something that also cyber criminals increasingly have on offer. Some, like the brains behind Emotet or QakBot, specialise systematically as access brokers in the penetration of IT networks. Other “service providers” take the knowledge and credentials obtained there and resell it. And even others, such as the groups behind LockBit 3.0 or Alphv, offer a sort of “ransomware-as-a-service” (RaaS), in which so-called “affiliates” then become active, without having to develop malware themselves.

These and other such services have come to cover virtually every aspect of a cyber attack and emulate economic trends in the outsourcing of tasks, but as opposed to the real industry, naturally without any legal underpinnings or regulatory bodies. Instead, established underground forums such as XSS and Exploit broker contacts to other cyber criminals. They offer them space to advertise their services or facilitate the deposit of guaranties in the form of cryptocurrencies. When conflicts arise, moderators act as arbitrators and pass binding judgements for the community, and in this sense are not unlike a court of arbitration. The deposited guarantees are then sometimes drawn upon for compensation. On this basis, cyber criminals can work together even under conditions of mutual mistrust.

ALL FOR MAXIMUM PROFIT

Even in the world of cyber crime, the objective of profit maximisation promotes innovation, efficiency and expansion. A clear example of this is that cyber criminals not only encrypt data they illegally gain access to, but they also publish it on dedicated leak sites to profit through so-called double extortion. This conduct was observed intensively for the first time with the attackers behind the ransomware Maze in November 2019.

By the end of 2021 double extortion had become the norm with ransomware attacks.

Another example is the modularisation of malware. With this, attackers can efficiently exploit new vulnerabilities in applications or systems, bypass improved detection methods countering such attacks, or even respond to the individual needs of their criminal users (“affiliates”). Emotet and QakBot, for example, were initially put to use as banking trojans, and later supplemented with modules to probe infected systems, to steal e-mail content, or to automatically send malware to other victims. Through modularisation, parts of software can be supplemented or revised, without having to modify the whole base code.

RANSOMWARE-AS-A-SERVICE AS ENABLER

To develop a kind of malware such as ransomware that can contend with modern countermeasures and analysis tools requires a considerable amount of technical knowledge in software programming. This isn't the kind of technical knowledge that can be found among all cyber criminals. And this is where ransomware-as-a-service comes into play. With ransomware-as-a-service, the demands on an attacker are lowered considerably, because nowadays, with the help of this service, even people who are technically relatively clueless can carry out ransomware attacks. By expanding to multiple attackers it also offers the advantage of becoming more difficult for affected parties to detect or differentiate between the approaches of individual affiliates.

ONE'S OWN REPUTATION AS CRITICAL RESOURCE

Cyber criminal groups indeed compete over their affiliates, which is why the reputation of one's own brand plays such an important role in the scene. This kind of rivalry leads to an increasing intensification of the threat situation. For example, a compelling argument for an affiliate is the amount of pressure that can be exercised on a victim. Which is why some RaaS providers such as Alphv (aka “BlackCat”) offer



DDoS attacks as extra service that can be deployed during the negotiation of a ransom. This way the competitive struggle between cyber criminal groups leads to a maximisation of pressure on victims.

Other characteristics that distinguish ransomware-as-a-service offers include the proportion of the ransom that is allotted to the affiliate, or the continuous improvement of the ransomware itself. Another ransomware-as-a-service that makes use of such “premium services” is LockBit, for example. They supply among others the malware StealBit, which specialises in the theft of data for blackmail purposes.

And even the “war for talent”, which the legal economy wages for the best in the market, can be found in the cyber criminal scene. Which is why a good reputation in one’s own circles plays such a key role there. Some forums for example only accept well-known or successful cyber criminals – and thus remain for the most part exclusive.

A QUESTION OF HONOUR

Trust – as strange as it may sound – is also a valuable currency even among cyber criminals. Should word get around after a ransomware attack that a decryption tool did not work “properly” or at all after a ransom payment was made, it would probably tend to lead to a failure in the receipt of future ransom payments as a consequence. All that would remain then as leverage would be the threat of publication of the data, but that rarely passes as something that builds trust. As such, the ability to display a minimum in good manners to their victims is also important for cyber criminals – here especially in the form of promises kept, data decrypted again, and no publishing of said data.

The BSI points out that payment of the ransom is never a guarantee that encrypted data will be released. Moreover, payment of ransom contributes to the flourishing of criminal ecosystems and to criminal organisations becoming larger and more professional. That is why the BSI recommendation

remains in effect: always refrain from paying the ransom. More important is to take effective precautions against ransomware attacks in the first place.

“TOO BIG TO FAIL” VS. “TOO BIG TO STAY AFLOAT”

Companies and institutions that are too large or too important to fail, are labelled “too big to fail”. Included among these during the global financial crisis in 2008, for example, were numerous banks, which could only be rescued from insolvency through state assistance. “Too big to fail” – does this also exist among cyber criminals?

To put it bluntly: No. Size is no reason for rescue here, but a reason for downfall. When a group of cyber criminals is successful, their public notoriety increases, and with that, also the kind of attention they get among security experts and law enforcement agencies. Which is why it has only been a question of time until such groups could be put out of business or have seen it as necessary to lie low:

- In January 2021 Emotet was taken down
- RaaS DarkSide disbanded after the cyber attack against Colonial Pipeline
- RaaS REvil disappeared after the cyber attack via Kaseya VSA
- The “Conti syndicate” fragmented in May 2022

Whereas in the industry, companies certainly do achieve the status “too big to fail”, cyber criminal groups tend to become “too big to stay afloat”. However, others will fill their vacant positions in due time – driven by greed for quick profits. ■

it-sa 2022 in Nuremberg

Cyber Security Finally Live Again: Review of Three Successful Expo Days

The it-sa Expo & Congress, Europe's leading exhibition on IT security, took place in Nuremberg from 25-27 October 2022. As conceptual sponsor of the expo, the BSI was on hand with a booth where people could ask technical questions and exchange ideas with BSI experts.

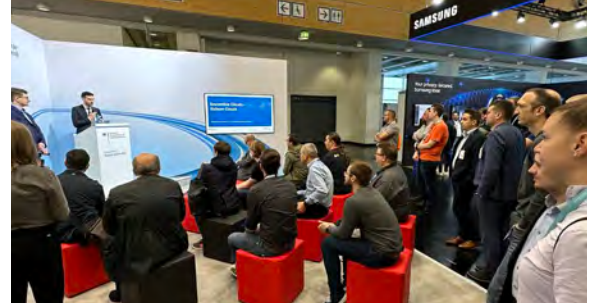
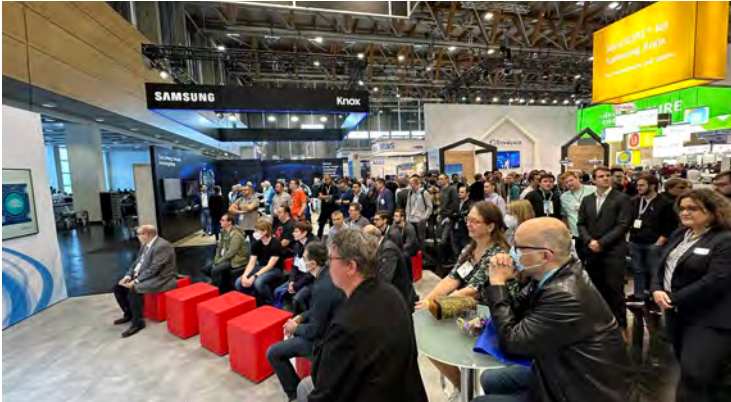


Numerous topics – lively interest

This year's main topics at the exhibition booth included the offering of the Alliance for Cyber Security, solutions for digital consumer protection and certification and media identities – and the interest among exhibition visitors was immense.



Certificate presentation for the tachograph card at the it-sa: Dr. Hans Hanauer, Managing Director of the company MaskTech International GmbH, and Sandro Amendola, BSI Director-General Standardization, Certification and Cyber Security of Telecommunication Networks



Speakers' Corner

The Speakers' Corner celebrated its successful premiere at this year's BSI booth. With their compact presentations on special topics various BSI experts offered insights into different aspects of cyber security.

“Report on the State of IT Security in Germany 2022” presented

At the it-sa, BSI Vice President Dr. Gerhard Schabhüser presented the current BSI situation report. The report summarises the IT security situation in Germany. During presentations, people on location had the opportunity to hear BSI data and insights on the cyber threat situation.



Presentation of the first copies of the BSI situation report: Prof. Dr. Roland Fleck, CEO Nürnberg-Messe GmbH; Roland Weigert, MdL, State Secretary Bavarian Ministry of Economic Affairs, Regional Development and Energy; BSI Vice President Dr. Gerhard Schabhüser; Peter Ottmann, CEO NürnbergMesse GmbH; Thomas Preutenborbeck, Member of Management Board NürnbergMesse GmbH

10 years Alliance for Cyber Security

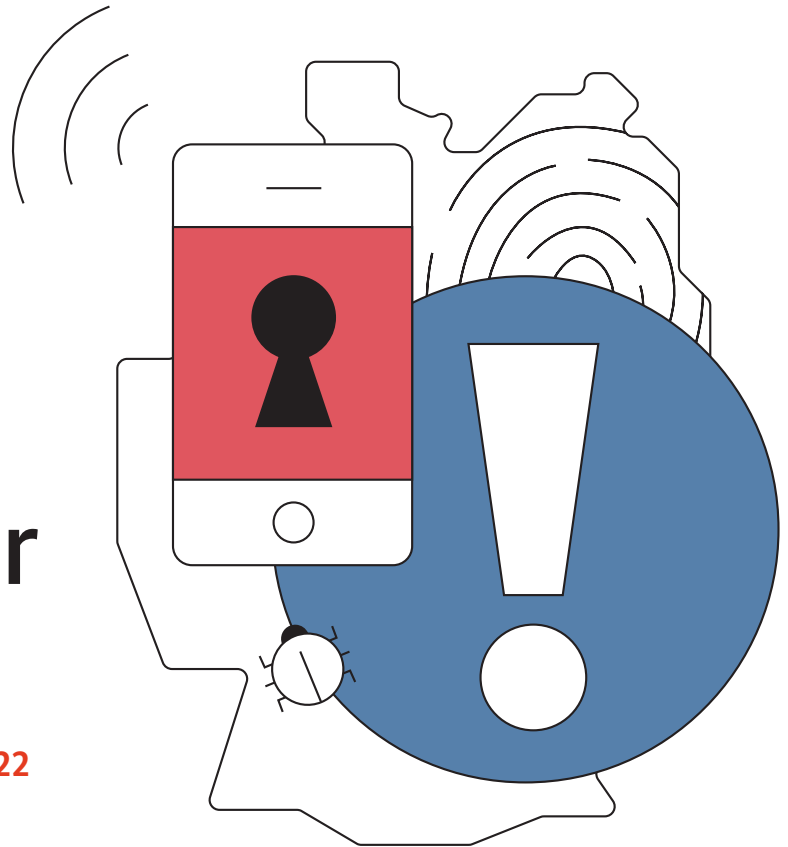
Europe's largest network for cyber security was dedicated its own area at the exhibition in honour of their anniversary.



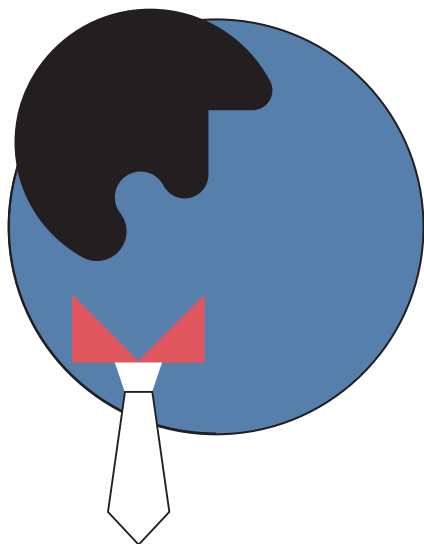
Save the date!
We're looking forward seeing you
at the next it-sa from 10-12 October 2023.

Threat Higher than Ever

The State of IT Security in Germany 2022



With the “State of IT Security in Germany 2022” report the BSI reports once a year provides information on the IT security threat situation in the reporting period. This year’s situation report clearly demonstrates that although the threat situation is very high, we are not completely at the mercy of the dangers.



CRITICAL SITUATION BECOMING MORE ACUTE

The already tense IT security situation in Germany worsened in this reporting period. With that, the threat in cyberspace is higher than ever. In addition to the ongoing threat of cyber crime, dangers from the Russian war of aggression against Ukraine were responsible. In Germany there was an accumulation of smaller incidents in connection with the war of aggression,

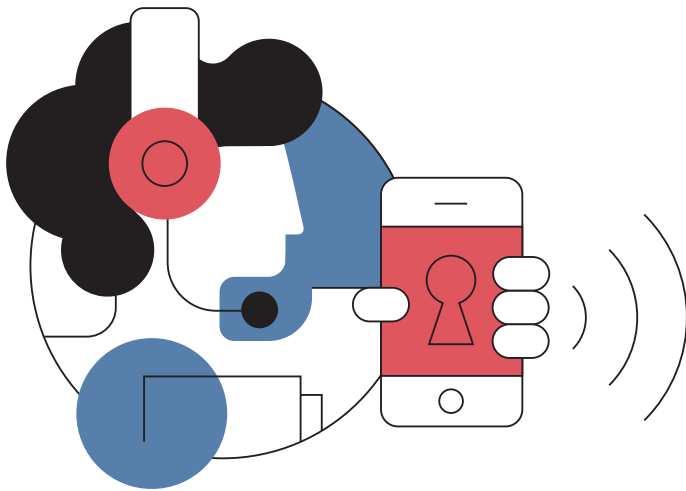
such as hacktivism attacks and disruptions to supply chains as well as an increased number of charity scam mails. A comprehensive attack campaign against German targets was not evident. Other NATO partners experienced serious consequences in cyberspace which, through the increased interconnectedness and globalisation, can be felt even across borders.

CYBER EXTORTION REMAINS ONE OF THE BIGGEST THREATS

The biggest threat currently in German cyberspace remains ransomware, particularly for businesses. Ransomware involves malware that uses encryption to prevent access to data and databases. Usually, attackers leave behind a ransom note, and often a demand for ransom money. The threat: Should the ransom money not be paid, the data is lost for the company. Threats are also made to publish sensitive data. In cases where this type of extortion is applied to high-revenue companies, it is called “big game hunting”. But ransomware attacks also pose a real threat to the administrative systems, as was the case in Saxony-Anhalt last year, for example.

FIRST DIGITAL STATE OF EMERGENCY IN GERMANY – BSI HELPS ON THE GROUND

In a district in Saxony-Anhalt in 2021 a state of emergency was declared for the first time after a ransomware attack on the district administration. The attack resulted in serious consequences: For 207 days no citizen services could be performed, such as payment of parental, social or unemployment benefits. The BSI deployed a mobile team to work on location, but also provided support from Bonn with further coordination of crisis management. In collaboration with Germany's armed forces the BSI analysed the attack and the software used and provided advice on rehabilitation and the security of the IT infrastructure.

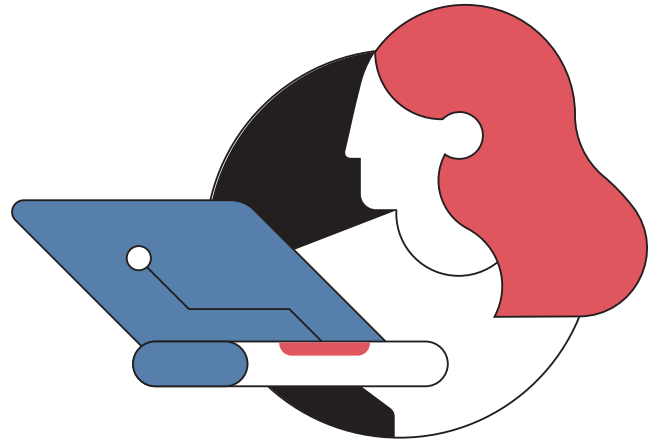


NUMBER OF VULNERABILITIES CONTINUES TO GROW

In 2021 The number of disclosed vulnerabilities in software products increased by ten percent in 2021 compared to the previous year. More than half of them exhibited high or critical scores according to the Common Vulnerability Scoring System (CVSS). Of all the vulnerabilities, 13 percent were rated as critical. Included among them was the vulnerability in Log4j, because it existed in many freely available software modules. For that reason people responsible for IT security could only estimate with difficulty whether the software they used exhibited the vulnerability. Due to the wide distribution of Log4j, an enormous attack surface for targeting from cyber attacks could be assumed.

CRIME IN THE INTERNET

For consumers, the biggest threats in the Internet are fake shops, sextortion, and identity theft. During the reporting period more than every fourth person was a victim of Internet crime. Here, it is notable that the numbers of third parties accessing online accounts and numbers of infections with malware decreased, however fraud in online shopping increased. Two out of five respondents say they were aware of security recommendations for protecting against Internet crime, but only slightly more than half actually put these



recommendations (to some extent) into practice. This indicates a need for more information, particularly since victims of Internet crime usually help themselves independently.

PROTECTION THROUGH PREVENTATIVE MEASURES

Globalisation, digitalisation and interconnectedness know no borders, which offers great opportunities, but also involves potential risks, as Russia's war of aggression against Ukraine currently makes us aware.

The past year has shown that unforeseen events can take the threat situation up to a new level, and collateral damage from cyber attacks in neighbouring countries can also have direct consequences for Germany. The report clearly shows: preventative measures are the most effective IT protection measures. Every computer that cannot be hacked, and every IT-based service that cannot be disrupted makes a crucial contribution to a functioning and digitally-interconnected society. ■



More information and subscription to BSI situation report:



The State of IT Security in Germany:
https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

The State of IT Security in Germany 2022

An Overview

Top 3 threats per target group:

Civil Society



Theft of identity data
Sextortion
Fake shops on the Internet

Economy



Ransomware
Vulnerabilities, unprotected or poorly secured online servers
IT supply chain: Dependencies and security

Government/Administration



Ransomware
APT
Vulnerabilities, unprotected or poorly secured online servers

First digital disaster emergency in Germany



207

 Days of digital emergency

Following a ransomware attack parental allowance, unemployment and social benefits, vehicle registrations and other citizen oriented services could not be provided.

The number of malware programmes is constantly rising.

The number of new malware variants has increased by

116.6

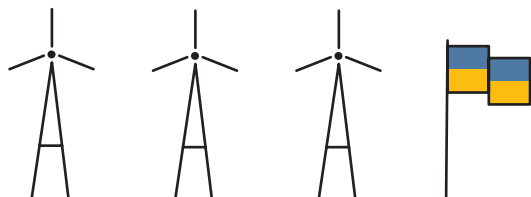
 Million in the current reporting periode.


Hacktivism in the context of the Russian war:

Mineral oil company in Germany must restrict critical services



Collateral damage

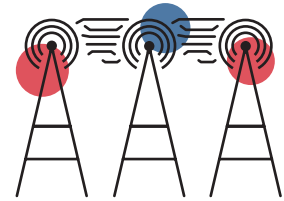
 after an attack on a Satellite Communication Company


20,174

vulnerabilities in software products (13% of them critical) were disclosed in 2021. This corresponds to an **increase of 10%** compared to the previous year.



15 Millions on malwareinfections in Germany were sent by the BSI to German network operators in the reporting period.



34,000

mails with malware were intercepted on average every month in German government networks



78,000

new websites were blocked from government networks because they contained malware.

69%

of all spam emails in the reporting period were cyber attacks such as phishing emails and email extortion



90%

of the mail fraud in the reporting period was finance phishing, i.e. the fraudulent mails gave the impression of having been sent by the banks.

BSI is the world's leading service provider in the field of Common Criteria certifications



5,100
2021

4,400
2020



Ten years of the Alliance Cyber Security:
by 2022, we are already

6,220
participants

Deutschland
Digital • Sicher • BSI

The #TeamBSI

Creators of Cyber Security

By Anna-Ris Kares, Division Human Resources Development



"In the BSI many different personalities, experiences and types of expertise come together. This is extremely important for us, because it allows us to consider our tasks from as many different angles as possible and find suitable solutions for everybody. This way, we learn from one another every day and make progress together as team."

Jennifer Breuer, Division Head DI 27
– Cyber Security in the Implementation of the Online Access Act

Motif from the #TeamBSI campaign – Jennifer Breuer

From information security consulting and digital identities right to cryptography and critical infrastructures (KRITIS): The tasks of the BSI are multifaceted, and through increasing digitalisation they continue to grow. With the implementation of the cyber security agenda of the Federal Ministry of the Interior and Community (BMI), the BSI is to take on even more tasks in future. For this, #TeamBSI is already equipped with substantial expertise – but is recruiting more professionals at the same time.

One thing counts above all at #TeamBSI: team spirit. To guide Germany on its path into a secure digital future, only together can we achieve our goals. Each and every one of us employees contributes our share.

To continue to master these tasks into the future, the team must grow – and do it in a market where especially in the IT area, the competition for talent is intense. Here, not only are the candidates for new jobs under scrutiny, but also increasingly the employers. With its online comments and reviews, the Internet is an important space for this. What that means for us as organisation is this: Promises we make to the outside world are promises we must also keep within our organisation. Of importance here is not just that we as the BSI can hire new employees who meet our requirements. It is just as important that we can also retain them.

COME TO STAY

In the race for the best talent, the BSI must also do some persuading as an employer. But, here is the good news: A lot of the best talent are already working for us. Not only does this manifest itself in the quality of our work, it also gives us a certain amount of leeway to hire graduates who may be motivated and qualified, but who still have little practical professional experience. We can fill the gaps in practical experience with our multifaceted advanced and further training offers – not only in technical terms, but also in terms of person development. In day-to-day operations our new colleagues can profit from the expertise of those who have worked many years at the BSI, and they will be trained as experts through practical experience on the job.

#TEAMBSI: DIGITAL COMPETENCE AND INNOVATION

At the focus of our #TeamBSI employer branding campaign are the aspects that distinguish us as agency and employer: team spirit and digital competence. In the campaign we are painting as broad a picture as possible of our many departments, tasks and target groups. We want to reach both university graduates as well as experienced experts who want to be part of creating information security in Germany and beyond. The #TeamBSI makes an enormous contribution to society as a whole for achieving secure digitalisation. With the campaign we not only want to present the BSI as employer, but also show the kind of exciting areas of work public service offers.

RETAINING EMPLOYEES THROUGH IDENTIFICATION AND STRENGTHENING INVOLVEMENT

In addition to exciting tasks and future-oriented projects, actively creating an issue that is so highly relevant for society is one of the biggest motivations for our employees and leads to a strong sense of identification with the BSI and its mission. Many of the colleagues in the different departments view their work not as job, but as vocation. It sounds strange, but it's true: The enthusiasm for the job and the tasks at the BSI is noticeable.

This atmosphere convinced us to involve our employees right from the start of concept development of our employer campaign. And, here is another topic we cherish: In #TeamBSI we believe in diversity. Our employees are no stereotypes, rather they are a colourful team. They are known for their different perspectives, characters and experiences of life that are so decisive for the togetherness in the #TeamBSI. That is why, with this campaign, we also hope to sharpen the awareness of this diversity, and contribute to a situation where all new and all current colleagues are not just “on hand”, but really feel like they belong. The great eagerness of the employees to get actively involved in person confirms us in this goal, which is directly reflected in our new employer image: We selected ten colleagues who share insights on their work world and illustrate how the BSI agency consists of such motivated and qualified people. In an authentic, sincere and spontaneous way, our protagonists tell of their experiences and encounters and how they feel about their work at BSI. ■

“With the implementation of the cyber security agenda of the BMI the BSI – as federal cyber security agency – will be given further tasks. For this, a strongly positioned BSI is required, with the requisite powers and a sufficient number of skilled professionals to be able to provide the necessary know-how.”

Dr. Gerhard Schabhüser, Vice President of the BSI

Further information:



Meet the #TeamBSI:
www.team-bsi.de

Want to help us shaping the digital world?

Join us in driving forward the secure digital future
and support the [#TeamBSI](#) with your commitment
and cyber security expertise.



More infos at:



Bundesamt
für Sicherheit in der
Informationstechnik

www.team-bsi.de

We are #TeamBSI: Dr. Friederike Laus

Dr. Friederike Laus works since September 2019 at the BSI and is currently officer in higher service in the Division Testing of Cryptographic Mechanisms. Her focus includes side-channel analyses, and in particular methods from the areas of machine learning and artificial intelligence as well as the cryptographic evaluation of messengers and audio and video conference solutions. We spoke to Friederike about her work and her involvement in the #TeamBSI campaign.



Motif from the #TeamBSI campaign – Dr. Friederike Laus

Friederike, how did you become officer for the testing of cryptographic mechanisms?

In a roundabout way: Originally, I applied for a position at the National Cyber Response Centre. They asked me there if I could envisage a job in the Division Cyber Security for Intelligent

Transport Systems and Industry 4.0. That sounded just as exciting to me, and so I started in this sector. Of course, I quickly realised that the work for me there, as a mathematician, was too applied. When an opening for a position in one of the two mathematics Divisions presented itself, I landed in the testing of cryptographic mechanisms, where I feel perfectly comfortable. Here, I can apply all of my abilities and expertise.

What embodies the team spirit the most for you at the BSI?

At the BSI there are a lot of colleagues who are technically extremely fit and enjoy sharing their knowledge with others. I know that I can turn to them at any time with questions, and naturally I enjoy helping them too, wherever I can – and not just internally in the Division, but also across sections and agencies. For me, this strong sense of collegiality combined with the high degree of technical expertise makes work at the BSI so special.

What motivates you in your work at the BSI?

What appeals to me the most is that I can work very close to the research level here at the BSI – similar to how I used to work as academic at the university. In our areas of specialisation we keep on top of research and developments to stay up

to date in the very fast-paced IT security branch, and do some research on our own, too. Whereas at university, one is often occupied with more theoretical topics, which perhaps may be put to use a few years later, here we work on highly topical subjects, which also always have a specific connection to an application.

Overall, I am very pleased to work for the BSI, and somewhat proud, to be part of such a competent and committed team. It fills me with satisfaction that I can make use of my abilities here so well and work together on something that benefits society, and not the interests of only a few. All of this motivates me tremendously to give all I have every day anew, and to contribute to making Germany a little bit more digital and secure. ■

Heighten Cyber Security in Local Governments

BSI Launches “Municipality Road Show” for Heightened Cyber Resilience in the Public Sector

By Division IT Security Consulting for State and Local Governments and Division National Liaison Office



It was the first time that a local government in Germany declared a state of emergency due to a hacker attack. The district of Anhalt-Bitterfeld saw no alternative. Its IT systems were so badly paralysed by a cyber attack in July 2021 that for at least a week it was not possible to pay out any parental, unemployment and social benefits. In order to heighten resilience against cyber attacks like this on the local government level, and to increase the degree of cyber security in general, the BSI initiated the “Municipality Road Show” digital event series.

Highly consequential cyber incidents like that which occurred in Anhalt-Bitterfeld generate uncertainty in many local governments as to whether their own IT infrastructures are sufficiently safe against cyber attacks. The accumulation of cases shows that in the area of local government agencies in particular, no uniform level of cyber security exists, or it is often inadequate.

The National Liaison Office – the point of contact of the BSI among others for federal agencies, states and local governments – and the BSI office of IT Security Consulting for State and Local Governments have taken note of these challenges, and that is why they developed the new Municipality Road Show format, specifically with local governments in mind.

SENSITISE LOCAL GOVERNMENTS TO IT SECURITY ISSUES

The basic idea of the Municipality Road Show is to hold a joint virtual event with interested states. The aim here is to sensitise local governments to the threats in cyberspace and to identify options to take action to heighten the cyber security level. The planning and execution of the event is done with the involvement of the states and the key local organisations. Among others, the BSI integrates into the format presentations from



the Divisions IT Security Consulting for State and Local Governments, National Liaison Office, CERT-Bund, BSI Standards and IT-Grundschutz. The states supplement this with different presentations tailored specifically to the state, to provide the local governments with recommendations for action, best practices, and case studies which would add value for their work in the area of IT security.

ORGANISATION AND PROGRAMME OF THE ROAD SHOW

As soon as a state announces an interest in holding a Municipality Road Show, one or more coordination meetings take place to organise the content and dates of the event together. Based on this, a joint invitation is prepared which is sent by the state administrations to the local governments of the respective state some four weeks before the road show is held.

During the online event, moderators address questions from the participants via a special chat system. At the end, selected questions related to the individual presentations are answered by the presenters. Questions that cannot be answered during the event are answered later in the FAQ and distributed to the participants together with the presentation slides.



The BSI contributes essentially the following items for the road show programme:

Keynote address from BSI senior management

With a keynote address the senior management underscores the significance of cyber security and sketches out the current challenges and threats.

Presentation: Threat situation and experience from ransomware attacks

In a presentation on the threat situation in local governments, the BSI contributes its experience garnered from working with ransomware incidents in the economy and administration. Along with this, an estimation of the threat situation is proffered, from which the imperative is derived to ensure suitable protection of the local government administrations. For this, the BSI presents preventative measures that go beyond baseline IT protection. And for situations in which an attack could not be prevented, the BSI presents reaction measures that are to be planned and prepared as preventative measures already before an attack.

Presentation: Information security for local governments

IT security is the prerequisite for successful digitalisation and should be implemented according to a holistic approach. In this presentation the BSI explains the steps and aids through

which a management system for IT security can successfully

be structured. Here, the BSI also goes into the IT-Grundschutz, the IT-Grundschutz profile “Local Government Baseline Protection”, and the support options of the Federal Cyber Security Authority.

Presentation: Online Access Act (OZG)

The OZG stipulates that all administration services across all states and administrative levels be connected over a portal network. With that, security risks within the network naturally potentially affect a large number of people, institutions and applications. To protect the network, the Federal Ministry of the Interior and Community (BMI) passed the “IT Security Regulation Portal Network” (ITSiV-PV) in January 2022, which also stipulates certain security standards for the local governments. In the presentation the BSI explains the requirements and protection measures.

Other offerings of the BSI

In this presentation the BSI exhibits a selection of products and offerings of the agency that are suited to enhancing the cyber security level of the local governments. This also includes participation in the Alliance for Cyber Security.

FIRST ROAD SHOWS IN SAXONY, LOWER SAXONY, SAXONY-ANHALT AND THURINGIA.

The first road show took place at the beginning of May in the Free State of Saxony where senior management and contact persons for information security from the local governments took part in the virtual event of the BSI and the Saxon State Chancellery. The significance of local governments in the cyber security architecture in Germany was also underscored by the participation of high-profile decision-makers from politics and economy. The kick-off was followed by road shows in Lower Saxony, Saxony-Anhalt and Thuringia, with steadily growing numbers of participants, which confirms the

enormous interest and need of the local governments for this subject area. For the first road show in Saxony alone, there were some 180 registrations. Beyond that, at the end of November, Municipality Road Shows took place with the states North Rhine-Westphalia and Mecklenburg-West Pomerania, with more planned for 2023. ■

The Perfect Couple: Information Security and Digital Administration

By Prof. Thomas Popp, State Secretary for Digital Administration and Administration Modernisation and CIO of the Free State of Saxony

Citizens as well as enterprises justifiably expect a modern administration to provide digital services reliably and securely. The more interconnectedly and digitally work is done, the more important the information security is. What is the Free State of Saxony doing in this regard?

More digital administration is a legitimate demand. This can only function, however, if we can guarantee the security of the data and the IT infrastructure. Prevention, emergency preparedness and assistance in emergencies are our daily business in the information security field. This applies to the state administration, and especially to the local governments. There, where a majority of the services for citizens and enterprises are provided, information security must definitely be emphasized.

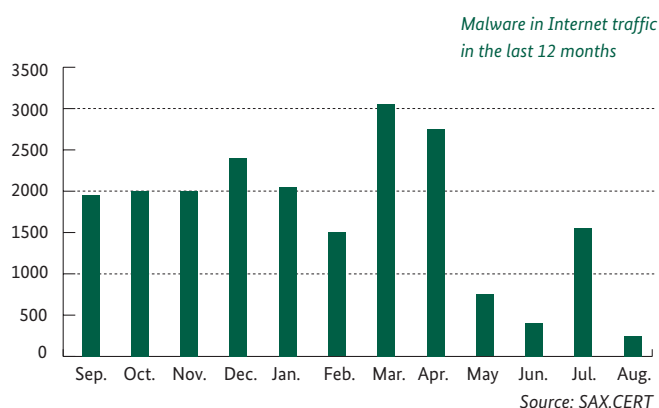
ALWAYS ROOM FOR MORE INFORMATION SECURITY

Naturally, there is no such thing as one-hundred percent protection. But, I am concerned that IT security is not pursued everywhere with the necessary vigour. The legal framework is available for this, however, with the IT Security Act which was passed in 2019.

It imposes certain obligations even on Saxon local governments. This includes for example the specification of an officer for IT security. Local governments are increasingly becoming the target of cyber attacks, in some cases with serious consequences. The more digital services that are provided, the larger the potential damage scenario will be. That is why we must now rethink. IT security is the compulsory insurance for critical infrastructures, to which – according to our understanding – local governments belong. This is precisely what the officer for IT security must actively take responsibility for in agencies and local governments.

IT SECURITY AS SERVICE

To support state offices and local governments in the daily battle against cyber criminals, the Saxon security emergency team SAX.CERT plays a key role. It analyses the state of information security and passes this information on to other parties. It evaluates numerous sources, particularly the central security systems of the Saxon administration network and the monthly security scans of more than 6000 web pages of the state and local government administration. Conclusions are drawn from this and measures derived to improve the security even more. Should an IT security manifestation or even an IT security incident take place, the SAX.CERT supports and advises the affected parties. All Saxon state and local government administrations are offered special services for cyber defence free of charge by the SAX.CERT. Included in this for example is an “intrusion sensor” for unauthorised accesses or an individualised vulnerability warning service.



Brief profile Prof. Thomas Popp

State Secretary for Digital Administration and Administration Modernisation and CIO of the Free State of Saxony

Thomas Popp was born on 8 November 1961 in Schweinfurt. He has worked in the Saxon State Chancellery since the beginning 2015, and presides over it since April 2018 as office head. Moreover, effective 1 August 2018 he was appointed as representative for information technology (Chief Information Officer – CIO) of the Free State of Saxony. On 20 December 2019 Thomas Popp was appointed as State Secretary and member of the Saxon state government.



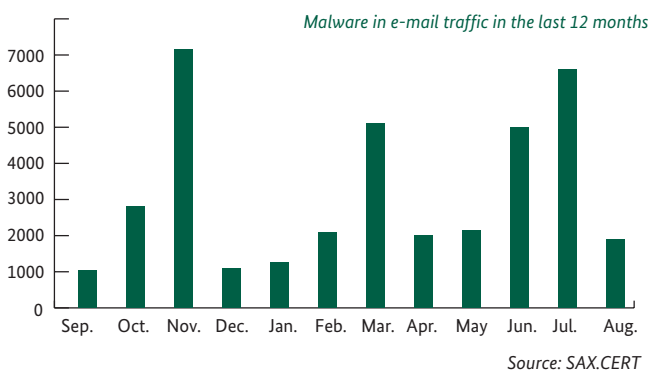
The Saxon State Secretary for Digital Administration and Administration Modernisation, Professor Thomas Popp (left), and the head of the Saxon security emergency team SAX.CERT, Prof. Dr. Karol Kozak, present in the innovation lounge at the ITOF their services for cyber defence, which all agencies and local governments can use.

ITOF – TOGETHER, DIGITAL, SUCCESSFUL

IT security was a topic of focus at the 10th IT and Organization Forum (ITOF), which was held in September at Dresden airport. Some 500 participants from Saxon state and local government agencies had an opportunity to find out in presentations, exhibitor booths and in the innovation lounge about how a secure digital administration works. The security emergency team SAX.CERT presented its services for cyber defence, such as the intrusion sensor HoneySense, a password checker, or web page scan. The ITOF is the leading internal administration event in the Free State of Saxony. It brings together state and local government representatives for an exchange of information.

THE HUMAN FACTOR

Technical security systems and specialists are two important pillars on which IT security rests. However, every civil servant in administration and every manager ultimately determines with his or her conduct the level of IT security. An attack is often successful because the human factor fails. If the technical security mechanisms symbolise the thick walls and the insurmountable moats, then the unthinking click on a link sent in an e-mail is the lever that lowers the drawbridge and thus offers the attacker the proverbial attack point.



Such things happen because cyber criminals understand how to exploit human traits such as curiosity or empathy and to manipulate their potential victims. That is why educating about risks and sensitising civil servants to more caution in the everyday digital life is essential.

For all civil servants of Saxon state and local government agencies we offer a free e-learning

programme for this. As of now it has been completed more than 17,000 times. Particularly popular is the event “The hackers are coming” – a vivid format that we offer often for our civil servants. Here, the dangers that lurk in the digital work environment, the damage they can cause, and how one can avoid them are all portrayed in an entertaining way. Some 15,000 civil servants have already taken part in this event.

Special event formats such as the BSI’s Municipality Road Show on 2 May this year also contribute to establishing awareness for IT security, particularly among local Saxon governments, and strengthen it even more.

SUMMARY

More digital administration is needed to be able to fulfil our mandate in future. A complex technical infrastructure and more digital networking in daily work routine help us achieve this. Of course, in the architecture of our systems and in daily work routine we must take care to ensure that IT security standards are met. We must make this a top-priority issue everywhere among management and work together on prevention and emergency preparedness. ■

Further information:



Home page SAX.CERT:
<https://www.cert.sachsen.de/>



How Photos for Your Identity Card Will Be Transmitted to Authorities in Future

Secure Electronic Transmission of Photos to Passport, ID Card and Foreign Authorities

By Ann-Kristin Derst, Joschka Olbrück & Sebastian Palm, Division eID Solutions for Digital Administration

How can biometric photographs be transmitted digitally in a secure way from a photographer to official agencies? The answer to this question is given in the technical guideline BSI TR-03170, “Secure Electronic Transmission of photographs to Passport, ID Card and Foreigners' Law Authorities”.

The “Act to Strengthen Security in the Passport, ID Card and Foreigners’ Law Document System” contains a series of new regulations on how electronic photographs can be securely transmitted to passport, ID card and foreign authorities. With this law, the Bundestag and Bundesrat intend to specifically counter the manipulation of photographs in particular on official documents through morphing. Morphing is an image manipulation technique in which the facial features of two or more people are morphed or merged into one single face in a photograph. With its publication in the Bundesgesetzblatt, the law has been in force since 11 December 2020.

The transmission of photographs as attachment of a De-mail has been regulated already since 2014 by the technical guideline TR-03146 (“E-Bild hD”). With the passing of PassAuswRÄndG, the BSI was commissioned to draft two further processes for secure transmission. One variant is the live enrolment stations in the offices of passport, ID card and foreign authorities.

These devices is regulated in the technical guideline TR-03121. Furthermore, transmission according to TR-03170 will also be possible, which is explained as follows:

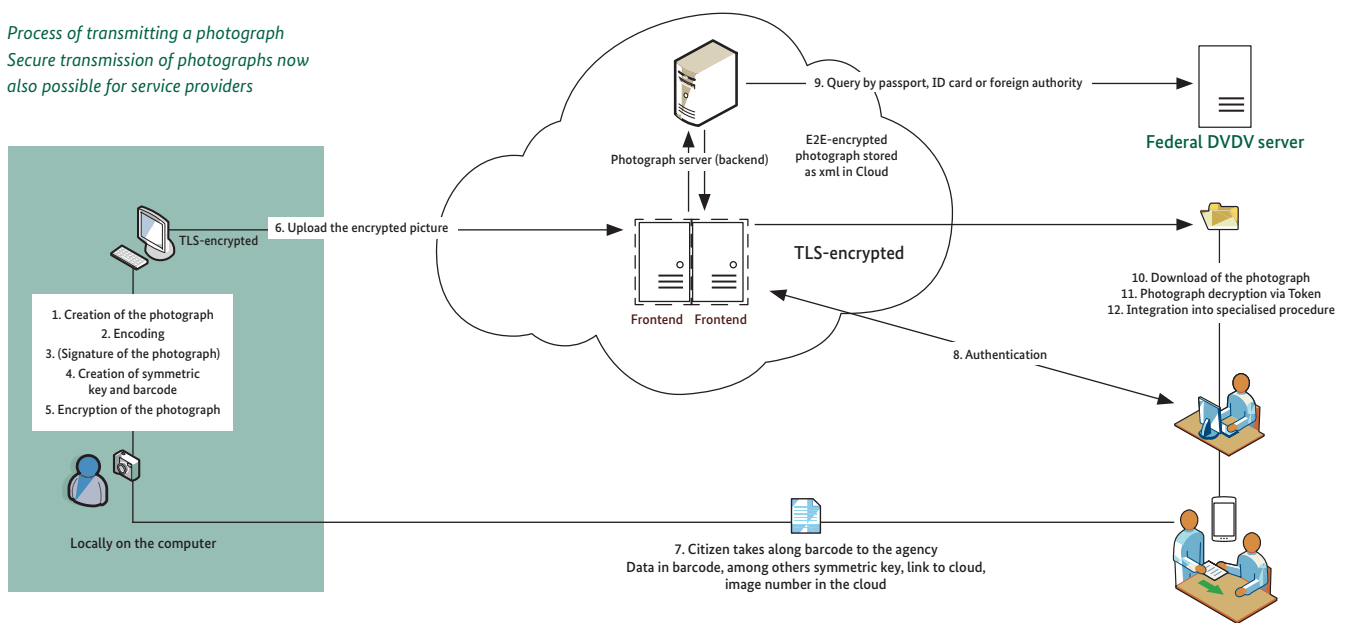
SECURE TRANSMISSION OF PHOTOGRAPHS FROM SERVICE PROVIDERS

The starting point for the new transmission process is service providers such as photographers who are to be able to transmit the photographs to a cloud service. For this, you must register at the cloud provider in advance, because only registered and verified service providers may transmit photographs this way. Moreover, only cloud services which are registered in the “Deutsches Verwaltungsdiensteverzeichnis” (DVDV) are given permission for transmission.

Digital transmission of photographs involves the following steps:

1. The citizen has a biometric photograph taken by a registered service provider.
2. In some cases the photograph is signed by the service provider.
3. Still at the service provider, a symmetric key and a barcode are generated for the photograph.
In addition to the symmetric key, the barcode also contains a unique identifier for the photograph and the URL of the cloud provider.
4. The photograph is encrypted with the symmetric key.
5. The service provider uses the upload interface to transmit the encrypted photograph to the cloud service.
6. The citizen receives a barcode from the service provider with which the ID document can be applied for at the agency.
7. The agency of passport, ID card or foreign authority calls up the electronic photograph at the cloud service using the identifier from the barcode.
8. With the help of the agency category, the cloud service checks at the DVDV whether the agency is authorised to do the call-up.
9. With that, the agency can authenticate itself vis-a-vis the cloud service.
10. The agency downloads the photograph.
11. Subsequently, the signature that may have been given by the service provider is verified and the photograph decrypted.
Decryption is only possible if the agency was given the correct key as part of the barcode.
12. The photograph is integrated into the agency's IT process for issuing the document.

*Process of transmitting a photograph
Secure transmission of photographs now
also possible for service providers*



The process enables flexible use of electronically recorded photographs from service providers by the agencies of authorities. Here it is important to note that citizens are not confined to a specific agency for calling up the photograph, but can choose these freely: This facilitates the calling up of the photograph from the authorised cloud service by every single authorised agency. This way, the same photograph can be used in multiple application processes, for example, as long as the deletion deadline of the photograph has not yet been reached.

Checking the authorisation of an agency at the DVDV ensures that the responsible agencies can call up and use photographs. The process also systematically makes use of end-to-end encryption. This guarantees that no changes can be made on the photograph after the upload. Besides that, even if the cloud

service were to be compromised, the photographs would be protected against unauthorised access this way.

The plan is to make the new process of secure transmission of their photographs available to citizens by 2025 at the latest.

Further information:



Technical guideline TR-03170:
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03170/TR-03170_node.html



More Security in Road Traffic

Cooperative Intelligent Transport Systems

By Dr. Katharina Bräunlich, Division eID Infrastructures for Digitization, and Torsten Matzerath, Division Cyber Security for Intelligent Transport Systems and Industrie 4.0

Connected driving and road infrastructures allow the development of new services and functionality. Such “Cooperative Intelligent Transport Systems” should contribute to shaping road traffic in a safer, more convenient and more efficient way. With the technical guideline BSI TR-03164, the BSI provides recommendations for secure operation of these systems.

In Cooperative Intelligent Transport Systems (C-ITS) road users and infrastructures to one another and exchange such messages. These Messages are used for example to warn against dangerous traffic situations or road conditions, and to regulate the flow of traffic. Emergency vehicles can use C-ITS to warn other road users when they are coming, so that vehicles can clear a corridor early on. It is also possible to switch traffic lights to green for emergency vehicles, to enable them to pass safely and without obstruction.

To allow vehicles or infrastructure components to make use of C-ITS, they must be furnished with dedicated hardware and software components, called C-ITS stations. Since these systems have such a large capacity to influence traffic safety and flow, attackers must not be able to manipulate C-ITS messages and thus gain control of traffic conditions. Otherwise they could, for example, warn against a hazard that doesn't really exist or imitate an emergency vehicle.

To prevent this, only sufficiently securely designed and correspondingly certified C-ITS stations may be used. Additionally, messages in C-ITS are digitally signed, because a digital signature and a public key infrastructure (PKI) guarantee the integrity of the C-ITS messages and the authenticity of the sender of a C-ITS message.

EU COMMISSION ENSURES STANDARDISED SPECIFICATIONS

With the help of the Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems, the European Commission has stipulated standardised specifications to guarantee both interoperability across all manufacturers and borders as well as a homogeneous security level. In addition to the European Certificate Policy, further specifications exist on the European level which substantiate the implementation of the specifications and which were developed by the European Telecommunications Standards Institute (ETSI).

However, the European Certificate Policy and the relevant ETSI specifications regulate certain areas in insufficient detail and completeness, because, for example, certain aspects or processes are not considered with sufficient precision, or not at all, or leave room for interpretation or leeway in design. This harbours a risk that the different stakeholders make assumptions in the implementation of operative C-ITS systems, which, under certain circumstances, don't take all security aspects sufficiently into consideration or which may put the interoperability at risk.



TECHNICAL GUIDELINE BSI TR-03164 CONTRIBUTES TO MORE CLARITY

In order to ensure more clarity and reliability here, at the beginning of 2022 the BSI published the technical guideline BSI TR-03164. It is to be viewed as supplement to the European specifications and pursues the objective of establishing a standardised basis for interpretation of the relevant specifications and supplying specific recommendations in cases where design leeway exists. With that, the technical guideline contributes clarity and interoperability between stakeholders from industry and the public authorities. The guideline also helps all involved parties to consider aspects of IT security right from the outset and thus to avoid potential vulnerabilities and to guarantee a homogeneous level of security.

The BSI guideline consists of two parts: The first part serves as guideline for secure operation of public key infrastructures for C-ITS. The second part fleshes out configuration, registration and operation of C-ITS stations.

SUMMARY

Cooperative Intelligent Transport Systems are currently being deployed. At this time, the first vehicle manufacturers and road infrastructure operators are beginning with operations of initial C-ITS services. With the fleshing out and specification of requirements on C-ITS in this early phase of development and with the technical guideline, the BSI wants to positively influence the implementation of operative C-ITS systems. In line with the “security by design” paradigm, security requirements are thus sufficiently addressed already before being introduced onto the market in series. This makes the system not only more secure, but should also have a positive effect on the rapid spread of C-ITS in traffic. ■

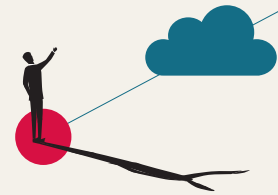
Further information:



Technical guideline TR-03164:
https://www.bsi.bund.de/DE/Service-Navi/Presse/Alle-Meldungen-News/Meldungen/TR_Transportsysteme_220117.html

BSI and NATO: Shaping Cloud Security in the Alliance

By Sven Niedtfeld, Division International Relations, and Division Virtualisation and Cloud Security



To fulfil its mission, the BSI also operates internationally. It cooperates bilaterally with numerous partner agencies in various countries and is well integrated in international organisations; NATO is among the most important ones. Within the defence alliance, the BSI currently contributes to actively shaping cloud security.

Towards NATO BSI takes on two roles for the Federal Republic of Germany: as National Communications Security Authority and as National Cyber Defence Authority.

In these roles BSI is directly integrated in a number of technically focused NATO committees and working groups. Furthermore, it fulfils an advisory function for the Federal Ministry of the Interior and Community (BMI) concerning cyber defence subjects in the policy context. Through its commitment in the western defence alliance, the BSI strengthens and enhances information security for the Federal Republic of Germany and its allies. Securing the exchange of information between the Allies is an essential precondition for NATO to stand for freedom and stability in the North Atlantic region in times of crises and conflicts.

The complexity of the alliance's structure is quite a challenge for all involved actors. NATO follows the principle that decisions need a consensus among the 30 member nations (32 after admission of Finland and Sweden) – even though there are sometimes divergent interests.

Its expertise and continuous involvement enables the BSI, even in this light, to set its own accents and to actively contribute to shaping the further development of information security. The preparation and adoption of the “Technical and Implementation Directive for the Protection of NATO Information within Public Cloud-based Communication and Information Systems” for “NATO UNCLASSIFIED” is an excellent example for that.

SECURE PUBLIC CLOUDS FOR NATO

For NATO, the digitalisation of its processes is highly important. The “NATO Cloud Computing Policy” specifies that suitable cloud technologies should be adapted in the alliance to support this objective.

In principle, special security requirements for information processing apply in NATO – depending on the classification level of the data. The lowest level is “NATO UNCLASSIFIED”, followed by the second classification level “NATO RESTRICTED”. There is no direct national equivalent in Germany for the former. Nevertheless, information of this level is only intended for internal NATO use and must be safeguarded correspondingly. “NATO RESTRICTED” is handled in the same way as the German “VS-NUR FÜR DEN DIENSTGEBRAUCH” (CLASSIFIED-ONLY FOR OFFICIAL USE). Thus, corresponding security requirements are considerably higher than for the first level.

The NATO “Information Assurance and Cyber Defence Capability Panel”, in which the BSI directly represents the interests of the Federal Republic of Germany, set up a project group – a so – called NATO Writing Team. Its objective is to identify and compile mandatory security measures for public cloud offers to qualify for the processing of “NATO UNCLASSIFIED” and “NATO RESTRICTED” information. The Writing Team comprises members from several NATO bodies and NATO nations. Besides Germany, France, Great Britain, and Belgium also take part in the Writing Team.



The BSI leads the activities of the Writing Team. Being the author of the internationally acknowledged “Cloud Computing Compliance Criteria Catalogue” (C5), it possesses precisely the right expertise for this role.

In December 2021, the Writing Team submitted the first results on schedule. It provided a proposal of the directive for processing “NATO UNCLASSIFIED” information in public clouds which was subsequently endorsed by the NATO nations. Since then, NATO has been capable of systematically approving public cloud services for the processing of “NATO UNCLASSIFIED” information. Taking the C5 and other current cloud standards into account, the directive reflects the current state-of-the-art in cloud security, and standardises internally as well as externally the security level of NATO when using public clouds.

HARMONISED SECURITY LEVELS AND THOUGHT LEADERSHIP

With the endorsement of this cloud directive for “NATO UNCLASSIFIED” by the NATO nations, the BSI succeeded in introducing the contents of the C5 standard into NATO policy, and harmonising the security levels of the two requirements specifications. This way, BSI exercises its role as thought leader in an international setting and successfully strengthens information security both nationally and within the alliance.

Another milestone will follow: Led by BSI, the Writing Team is now working on expanding the existing directive to “NATO RESTRICTED”, enabling NATO to also process information of this classification level in public clouds in the future. ■

Further information:



Cyber defence topic at www.nato.int:
https://www.nato.int/cps/en/natohq/topics_78170.htm



C5 cloud computing criteria catalogue:
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html



Update for European Cyber Security

By Joshua Breuer and Samuel Rothenpieler, Division International Relations

On 16 December 2020 the European Commission announced its proposal for the NIS-2 Directive (NIS2), in which minimum cyber security requirements on listed entities and Member States are defined. Since then, intensive negotiations have taken place in both the Council of the European Union as well as in the European Parliament. On 12 May 2022, in the third political trilogue, an agreement could be reached between the chief negotiators from Commission, Parliament and Council. With that, all that is left to do in coming weeks is to officially adopt the Directive.

NIS2 is to replace the NIS Directive from the year 2016 (NIS1), in which for the first time a uniform legal framework for EU-wide build-up of national capabilities for cyber security, stronger cooperation of EU Member States (MS), as well as minimum security requirements and reporting obligations for operators of critical infrastructures and for certain providers of digital services were established.

Already early on there were indications that the Commission, in the framework of the established review, intended to achieve further harmonisation. The different approaches to identification in particular, led to discrepancies among the EU Member States in the number of entities listed, and with that, also in the volume of reporting. Moreover, the level of security requirements was unequal.

CONTENT OF THE AGREEMENT

Consequently, NIS2 induces extensive changes: The scope of application is expanded in terms of quality and quantity. In this respect the Directive incorporates additional sectors; for the first time public administration entities are included. As a rule, the listing of entities within the sectors in future is done based on their size (“size-cap rule”). In the implementation, however, the Member States have a certain amount of leeway. The Directive differentiates between important and essential entities,

whereby the latter are subject to stricter oversight, and the security requirements can be applied on the national level in a graduated way based on an evaluation of proportionality. The compulsory security measures are listed in a catalogue which, compared to NIS1, also includes new requirements, such as supply chain security.

The reporting obligations were adapted, as well: The current single-tier reporting obligation for incidents is replaced by a three-tiered reporting regime with fixed deadlines.

Aside from that, new topics are formally transferred to European cooperation formats, such as the coordinated vulnerability disclosure as well as a European vulnerability database. In NIS2 there are also regulations for cyber security crisis management. In addition to the groups already established (CSIRTs Network and Cooperation Group), the “European cyber crisis liaison organisation network (EU-CyCLONe)” is legally implemented.

BSI AND NIS2

NIS2 will also lead to a considerable expansion of the listed entities in Germany. The BSI is in favour of continuing to nationally take into account the BSI Kritis Regulation. For the BSI, the area of supervision and enforcement also plays an important role. Here, the powers and possibilities for action

REGULATORY AREA

CAPABILITIES OF EU MEMBER STATES

- National CS authorities
- National CS strategies
- Framework for coordinated vulnerability disclosure
- National framework cyber security crisis management

RISK MANAGEMENT

- Accountability for top management
- Obligatory security measures for “essential” and “important” services
(* new category)
- Obligatory incident reporting

COOPERATION & EXCHANGE OF INFORMATION

- Cooperation Group
- CSIRTs Network
- EU-CyCLONe
- CVD and Europ. vulnerability registry
- Peer reviews
- ENISA report on the state of cyber-security in the Union

Source: DG CNECT

for the national competent authorities will be expanded. However, for BSI the tasks will likewise increase substantially when it comes to advice and support.

As Federal Cyber Security Authority, in the course of negotiations the BSI actively contributed its expertise and the experience it derived from NIS1, and helped achieving a positive result for the benefit of cyber security.

IMPLEMENTATION AND FURTHER LEGISLATIVE CONTEXT

After official adoption of the new Directive, there follows a 21-month period for implementation in national law. It is already foreseeable that changes in the BSI Act will be necessary in Germany, since requirements of the Directive considerably exceed provisions of the IT-SiG 2.0, or in some cases replace them.

As so-called horizontal legal act, the NIS2 establishes an inter-sectoral minimum security level, however in view of further sectoral and horizontal legal acts, clear cross-references to other regulation areas ensue. At about the same time the Critical Entities Resilience Directive (CER) was negotiated, which includes a revised concept for the resilience of critical infrastructure and whose listed entities are to be automatically defined according to the NIS2 as essential entities. Also, the

Digital Operational Resilience Act (DORA) for regulating the financial sector includes provisions for identification, supervision and enforcement in the area of IT security of financial entities, which likewise must be taken into account in the national implementation of the NIS2. Another important building block of European cyber security legislation which is currently being negotiated addresses the cyber security of institutions, bodies and agencies itself that do not fall under the scope of NIS2 and are still not subject to coherent regulation. ■

Further information:



Press story on NIS-2 Directive:
https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985



Press story on NIS-2 Directive:
<https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/>

Security Rather than Risk

How Digital Consumer Protection in the BSI Improves the Security of Consumer Data

By Jasmin Henn und Katarina Kühn, Division Secure Consumer Products and Services, Market Monitoring



The BSI regularly registers reports on data leak incidents, which refers to unauthorised access and disclosure of data that is not intended for third parties. What is revealed here is the often inadequate implementation of appropriate requirements on the security of the information technology.

Data can be found everywhere in the world. Consumers can profit from the spread of digital, data-driven business models and the increasing interconnectedness of information technology systems if they are looking for such digital products and services. What is often neglected, however, is a differentiated approach to data, particularly when taking the damage potential into consideration, should misuse occur. For consumers, generally a risk exists that the personal data they supply and is stored at online services can be stolen by unauthorised individuals and used for future attacks, such as phishing or smishing.

Data leaks are often connected with ransomware attacks. This was how cyber criminals succeeded in gaining access to the IT infrastructure of a German travel company in October 2021. It resulted in the encryption of sensitive data by ransomware, accompanied by the theft and publication of part of this data. Among others the attackers disclosed passport information of customers from Germany. The BSI is increasingly also seeing the unintentional disclosure of sensitive data due to a lack of adequate protective measures, resulting in sensitive data (often private) finding its way into the public sphere without the involvement and in many cases without knowledge of the affected parties. Attacks on customer databases at online services such as online shopping, for example, often lie outside of the sphere of influence of the affected consumer to do anything about it. That is why such security incidents with

their resulting publication of sensitive private data particularly undermine trust in the use of digital services as well as digitalisation as a whole.

STRENGTHENING THE DATA SECURITY OF CONSUMERS

Digital consumer protection is a statutory mandate of the BSI. In this framework the BSI is committed to safeguarding consumer interests and information security for consumer data vis-a-vis manufacturers and providers. An important tool for fulfilling this mandate is the systematic observation and evaluation of IT security incidents where consumers are affected. For this, the BSI commissioned a detailed study of the security of consumer data in databases of online shopping platforms. The goal of the study was to gather information; on one hand regarding the security of customer data on the typical online shopping platforms in the market, and on the other hand regarding the specific needs, expectations, perceptions and conduct of consumers when actual incidents of data leaks occurred. In vulnerability analyses and security tests a selection of software solutions for online shopping (shop software) was examined. The vulnerabilities discovered here are dealt with by the BSI in the framework of the usual coordinated vulnerability process. Moreover, interviews were held with experts on the subject of data security in online shopping. Through the questions, important insights could be obtained for effective measures in digital consumer protection, particularly in online shopping.



Andreas Sachs
Branch Head Cyber Security and
Technical Data Protection
Vice President
Bavarian State Supervisory
Authority for Data Protection

*“From the point of view of the consumer,
there is not much more one can do.
After all, it is the online shops’ job
to ensure sufficient security.”*

DATA SECURITY AS COMMUNITY TASK

The results gathered from the study so far indicate that it is essential that software producers promptly provide security updates for any IT security holes of the shop software used that are identified, and that they are also just as promptly installed by the operators of the online shop themselves. In addition to the producers and the providers, also the consumers can make a certain contribution to raising data security. In the aforementioned study, the experts that were interviewed explained some steps that could be taken, such as selecting secure and different passwords to protect different accounts. The necessity that consumers ensure they have a secure password management system, but also the responsibility of the operators of online shops was emphasized by Andreas Sachs from the Bavarian State Supervisory Authority for Data Protection. The full results of the study are anticipated to be published at the beginning of 2023.

Whether on an ongoing basis or for specific events, in dialogue with producers and providers the BSI works to ensure that digital consumer products and services provide a minimum level of information security. Even the national IT Security Label of the BSI pursues the goal of enhancing the IT security level of consumer-related IT products and services. In future the BSI will be publishing further product categories. On top of that, there is a focus on sensitising consumers regarding the use of secure passwords, the utilisation of a password manager, and the application of two-factor authentication. Here, digital consumer protection always has its three key objectives in focus: to sharpen the risk awareness of the target group in digital environments, to strengthen their judgement, and to enhance their problem-solving skills. ■



Dr. Ayten Öksüz
Officer for Data Protection and
Data Security
Consumer law group
Verbraucherzentrale NRW e.V.

*“Passwords are important, too: If a person
chooses the same password for multiple
accounts, then if attackers have the e-mail
address and the password from a shop
account, for example, they can first see if
they can use this combination to get into
the e-mail account of the affected person. If
successful, they would gain access to a lot of
sensitive data. Access to e-mail content, but
also to contact lists – and then launch further
phishing attacks, for example*

Further information:



Protection against phishing and smishing:
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html



Register a vulnerability:
https://www.bsi.bund.de/EN/IT-Sicherheitsvorfall/IT-Schwachstellen/it-schwachstellen_node.html



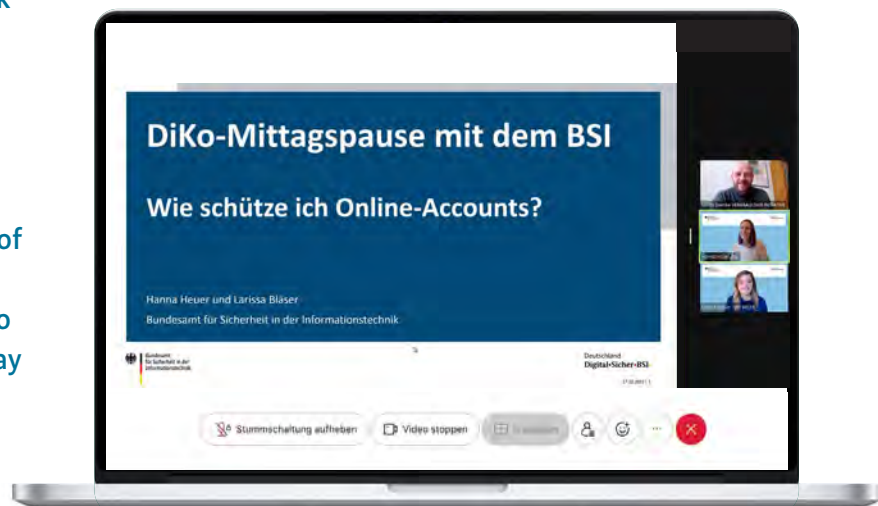
The IT Security Label of the BSI:
https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/IT-Sicherheitskennzeichen/it-sicherheitskennzeichen_node.html

Helping Older People Live a Secure Everyday Digital Life

Target Group-specific Sensitiation in Digital Consumer Protection

By Hanna Heuer, Division Cyber-Security for Society and Citizens

“I don’t know enough about that, I always ask my daughter.” Or: “My grandson set that up for me and it’s marvellous. Now we can see one another over video on the smartphone.” For staff at the BSI, such statements are common for example when they present the BSI’s offering to consumers on the open day of the German Federal Government in Berlin in summer. One of the tasks of the BSI is also to assist older people in organising their everyday digital life more securely.



People over 60 are happy to make frequent use of new ways to communicate over mobile devices or applications on the Internet. However, many of this generation don’t always feel safe when using devices and applications.

Once a year in the Digital Barometer, the BSI and Police Crime Prevention of the Federal States and the Federal Government ask citizens in a representative online survey about their perceptions and experiences related to cyber security and criminality. Emerging from the current Digital Barometer 2022 is information about whom older people turn to with their questions about this: 44 percent indicate that they receive help from family, friends and acquaintances. Roughly just as many (48%) research their questions on the Internet. At the same time, a higher degree of security consciousness is evident in this age group, which, compared to younger people, makes more use of security measures. For example, they activate automatic updates for their smartphone more frequently.

A LOOK AT LIVING ENVIRONMENT

Among others, such findings raise questions about how the information and advisory services of the BSI that are aimed expressly at private users should be designed, to get through to even more people about digital consumer protection. It is one of the BSI’s goals to raise the sensitivity of consumers to information security. If the aim is to address a target group of people over 60 years old, it makes sense to work together with organisations or existing projects that are already associated with the target group and are aware of their living environment and needs. This way, security awareness can be raised using a cooperative approach.

Further information:



Digital Barometer 2022:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/Digitalbarometer-ProPK-BSI_2022.html



LUNCH BREAK WITH THE BSI

Against this backdrop, in 2022 the BSI expanded the cooperation with the “Digital Compass”, an initiative that is supported by the German National Association of Senior Citizens' Organisations (BAGSO) and “Deutschland sicher im Netz” (DsiN, an initiative to contribute to greater IT security) in partnership with the Consumer Initiative (Verbraucher-Initiative), and is funded by the Federal Ministry for the Environment, Nature Conservation, Nuclear Safety and Consumer Protection (BMU). The Digital Compass is a meeting place for questions related to the Internet, and among others provides free offers for seniors – on location and at roughly 100 sites around Germany, as well as online.

Involved with the Digital Compass are so-called “Internet pilots”, who help older people try out and explore the Internet. It is precisely these Internet pilots who are the target group of the online event series “Lunch break with the BSI”, which was held in spring and autumn of 2022 with three instalments each. In addition to actual incidents related to a specific subject area, the BSI staff presented recommendations on this topic and gave instructions as to what in particular – under the aspect of IT security – must be considered. Here, topics ranged from secure settings on the home router, to backups for data

protection and measures for account security, right to tips for safe online shopping for Christmas. Equipped with this knowledge, as multipliers the Internet pilots can spread the recommendations of the BSI in future.

FURTHER COLLABORATIONS

In addition to working together with the Digital Compass in various forms already since 2019, the BSI is also in constant contact with the BAGSO. For example, for the revision of the BSI’s “Guides to everyday digital life” brochures, the organisation supplied older test readers who gave helpful feedback on the intelligibility of the copy. Moreover, last year the BSI participated in BAGSO’s German Seniors’ Day, which, because of Corona, could only be held in digital form.

These and other measures help establish the BSI as advisor for more security in everyday digital life among older people, and to strengthen precisely here the role of the Federal Cyber Security Authority. And not just in the form of knowledge that older people acquire, rather in a very practical sense, such as when they directly change the settings on their router during a workshop – and with that, don’t have to wait until the next visit of the daughter or grandson. ■



Guides to everyday digital life (only on German available):
https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Broschueren/broschueren_node.html

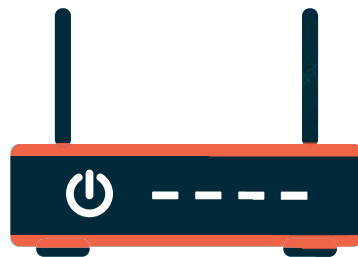


Digital Compass:
www.digital-kompass.de

Nine Tips for a Secure Home Network

Solid Protection for the Router - the Heart of the Digital Home Network

The router is the heart of the digital home network. It acts as junction for all network-capable devices – computers, mobile devices, smart TVs and smart household appliances – both for the Internet as well for one another. As central interface between the Internet and the home network, it is incredibly important to protect the router against unauthorised access and attacks from outside.



In an unprotected state, routers are a gateway for cyber attacks. If an attacker succeeds in penetrating the router, they can compromise the device itself along with all connected devices and cause personal or financial harm to the users:

Data theft: Attackers can spy out private data, passwords or e-mails. This means they can also steal online shopping login information or credit card data.

Misuse the telephone line: From within the network, attackers can dial numbers that are liable to fees or make high-priced calls abroad at the expense of the connection holder.

Spy on web activities: Since the router processes and documents all Internet traffic in the network, attackers can spy data and all information about visited web pages and services used – and for all the devices in the network.

Misuse Internet access: Hackers can use third-party networks to call up or distribute illegal content or to attack other Internet users. For this, the router is integrated into a botnet and used for distributed denial-of-service (DDoS) attacks or to send spam, for example.

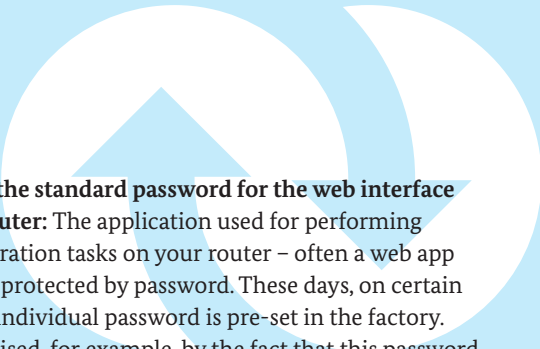
Install malware: Router hacking is often only the first step of more advanced attacks. After hacking the router, attackers can install malware and prepare for further cyber attacks.

Attack devices in network: A hacked router can be the starting point of further attacks on devices in the network. This means that every device connected to the router is a risk.


Replace firmware: Attackers can replace the firmware installed on the router or infect it with malware. After that, the router doesn't work anymore as it should, can be controlled externally and is vulnerable for future attacks or spying activities.

HOW TO PROTECT YOUR ROUTER

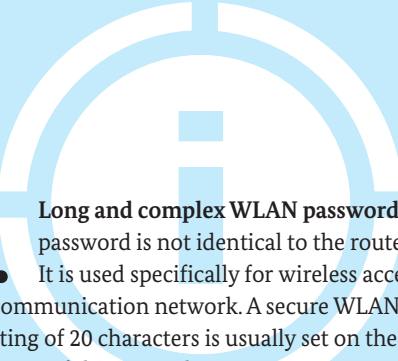
The most important thing anyone who wants to protect their home network and all connected Internet-capable devices must do is set up their router securely, and safeguard it properly. With the following nine basic tips you can lay a solid foundation for secure operation of your (W)LAN.




1. Replace the standard password for the web interface of the router: The application used for performing administration tasks on your router – often a web app in the browser – is protected by password. These days, on certain router models, an individual password is pre-set in the factory. This can be recognised, for example, by the fact that this password is described as “individual” in the user manual. Nevertheless, there are still routers that are shipped out with standard passwords, such as “admin” or “1234”. It is imperative to change these access codes immediately, because even attackers know (and use!) these standard passwords. The BSI recommends passwords consisting of a minimum of eight characters as well as different character types such as upper and lower case letters, digits and special characters.



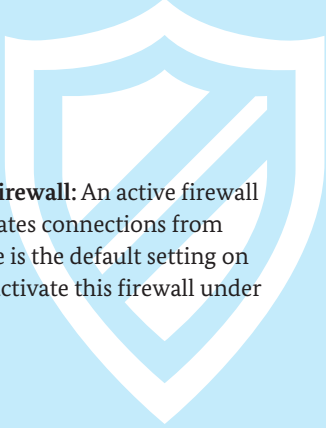
2. Replace the standard network name: The name of the WLAN on some routers contains detailed information about manufacturer or model of the device. For potential attackers, this information can be useful and should be changed.



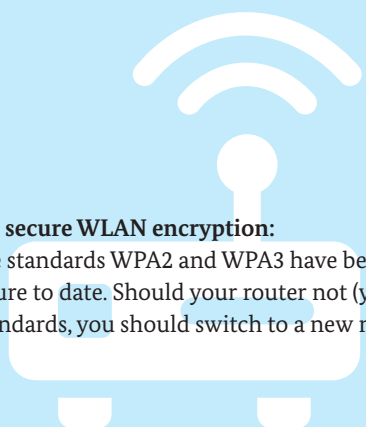
3. Long and complex WLAN password: The WLAN password is not identical to the router password. It is used specifically for wireless access to the local communication network. A secure WLAN password consisting of 20 characters is usually set on the router in the factory. If this is not the case on your router, assign a password made up of more than 20 unrelated characters, consisting of the four types of characters specified above.



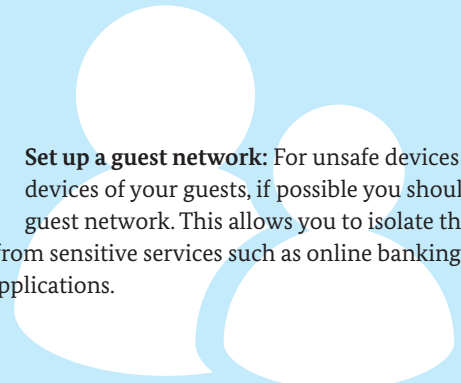
4. Keep the firmware up to date: Software updates are important because they rectify known security holes. If possible, activate automatic installation of software updates, because this will give you a high level of convenience and security. Check for updates regularly yourself if this option is not available.



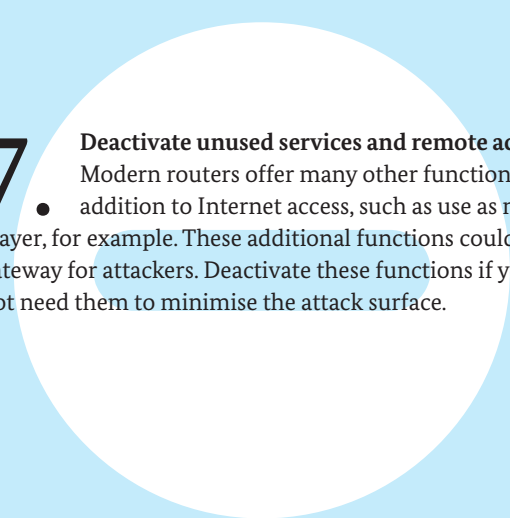
5. Do not deactivate the firewall: An active firewall that controls or deactivates connections from the outside to the inside is the default setting on many routers. You should not deactivate this firewall under any circumstances.



6. Use secure WLAN encryption: The standards WPA2 and WPA3 have been considered secure to date. Should your router not (yet) support these two standards, you should switch to a new model.



8. Set up a guest network: For unsafe devices or for the devices of your guests, if possible you should set up a guest network. This allows you to isolate these access points from sensitive services such as online banking or home office applications.



7. Deactivate unused services and remote access: Modern routers offer many other functions in addition to Internet access, such as use as media player, for example. These additional functions could be a gateway for attackers. Deactivate these functions if you do not need them to minimise the attack surface.

9. Note the IT Security Label: Router suppliers can get the BSI IT Security Label for their products. Requirement for this: They guarantee that their product possesses certain security features. If you are planning to buy a new router, uses this label (see below for info) as purchase criterion.

Further information:

Transparent security through the IT Security Label: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/IT-SiK-fuer-Verbraucher/IT-SiK-fuer-Verbraucher_node.html



WLAN – what you should know: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/WLAN-LAN-was-man-wissen-sollte/wlan-lan-was-man-wissen-sollte_node.html



Security tips for using private and public WLAN https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Router-WLAN-VPN/Sicherheitstipps-fuer-privates-und-oeffentliches-WLAN/sicherheitstipps-fuer-privates-und-oeffentliches-wlan_node.html



Creating secure passwords: https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html



Fact sheet “Secure Passwords”:
<https://www.bsi.bund.de/dok/409620>



THE IT SECURITY LABEL FOR ROUTERS

With the German IT Security Act 2.0, the BSI received a mandate from legislators to introduce an optional IT Security Label (IT-SiK), which is also issued for routers. For consumers the IT Security Label establishes transparency by making the basic security features of IT products recognisable at a glance. With the IT-SiK, users can inform themselves about security functionality that is warranted by manufacturers.

Order your BSI Magazine



Bundesamt
für Sicherheit in der
Informationstechnik

Federal Office for
Information Security (BSI)
Division Public Relations

P.O. Box 20 03 63
53133 Bonn
Phone +49 (0) 228 99 9582 5455
Fax 0228 99 9582-5455
E-mail: bsi-magazin@bsi.bund.de

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 editions directly by mail following publication in June and in December 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, House No.

Postal code, City

E-mail

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 20 03 63, 53133 Bonn, Germany, is responsible for processing your aforementioned personal data. The data 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 e-mail to bsi-magazin@bsi.bund.de. Revoking consent does not affect the legality of prior processing done before revocation. For more information on how we process your personal data and what rights you are entitled to, please refer to the “Privacy policy” attached for ordering BSI publications. Simply send in the form by fax or e-mail:

Fax: +49 (0) 228 99 9582 5455 | E-mail: 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 to: bsi-magazin@bsi.bund.de.

Privacy policy

https://www.bsi.bund.de/EN/Service/Datenschutz/datenschutz_node.html

Legal Notice

Published by:	Federal Office for Information Security (BSI) 53175 Bonn
Source:	Federal Office for Information Security Division Public Relations Godesberger Allee 185-189 53175 Bonn Phone: +49 (0) 228 999582-0 E-mail: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Last updated:	December 2022
Content and editing:	Katrin Alberts, Sonia Golás, Mark Schulz, Federal Office for Information Security; FAKTOR 3 AG, Kattunbleiche 35, 22041 Hamburg, www.faktor3.de
Concept and design:	Federal Office for Information Security
Printed by:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe www.ak-druck-medien.de
Item number:	BSI-Mag22/716-1e
Image credits:	Title: AdobeStock © sasun Bughdaryan; p. 03: BSI; p. 04 – 05 (from left to right): BSI, AdobeStock © sasun Bughdaryan, BSI, AdobeStock © metamorworks, AdobeStock © jozefmicic, AdobeStock © insta_photos; p. 06 – 07: BSI, BSI, BSI, AdobeStock © BAIVECTOR; p. 8 – 9: AdobeStock © Open Studio; p. 10 – 11 AdobeStock © Meawstory 15Studio; p. 12 – 13: Schloß Elmau, BSI; p. 14: BSI; p. 15 (top): Federal Government/Güngör, p. 15 (bottom): BSI; p. 16 – 17: BSI; page 18 – 19: AdobeStock © sasun Bughdaryan; p. 20: AdobeStock © sasun Bughdaryan; p. 22 – 23: AdobeStock © whyt; p. 24: AdobeStock © sasun Bughdaryan; p. 27: AdobeStock © samuii, AdobeStock © sasun Bughdaryan; p. 18 – 27 (background graphics): AdobeStock © lil and AdobeStock © Peter Kögler; p. 28 – 29: BSI; p. 30 – 31: Koivo c/o kombinatrotweiss.de; p. 32 – 33: BSI; p. 34: BSI; p. 36 – 37: BSI; p. 38: BSI; p. 39: AdobeStock © Parradee; p. 41 (left): Matthias Rietschel, p. 41 (right): Annett Weigelt; p. 42: AdobeStock © 4zevar and AdobeStock © Daniel Berkmann; p. 43: BSI; p. 45: AdobeStock © metamorworks; p. 46 – 47 (illustration): AdobeStock © jozefmicic, p. 47 (photo): Thomas Caspers; p. 48 – 49: AdobeStock © rawku5; p. 50: AdobeStock © New Africa; p. 51 (left): Private, p. 51 (right): © Verbraucherzentrale NRW; p. 52: BSI; p. 53: AdobeStock © insta_photos; p. 54: AdobeStock © pixelalex; p. 55 – 56: AdobeStock © Matthias Enter

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>

Follow us:



