Federal Office
for Information Security

The State of IT Security in Germany 2017

Foreword

Nothing is as constant as change. Heraklit's realisation hardly fits better to anything than digitalisation. Its opportunities for our social, scientific and economic progress are immense. But so are the risks that have to be kept under control.

A look into the past shows: the last few years have been characterised by IT security incidents as never before. Despite all efforts, they occurred on a daily basis and were seldom limited to Germany. Hospitals in the United Kingdom were affected, energy suppliers in the Ukraine, one of the largest global logistics companies, banks, pharmaceutical companies and steel producers – these are just a few victims of the most recent cyberattacks. Cyber crime, cyber espionage against governments and economies as well as provoked failures of critical infrastructures are serious threats for our 21st-century society.

However, it is also evident: never before have we enacted so many laws and achieved so much in the area of IT and cyber security as in the past few years. Never before have we been involved in so many international dialogue and exchange formats concerning IT and cyber security. The help of a new cyber security strategy initiated by the Federal Government creates a strategic framework for all activities in the area of cyber security. The BSI has evolved into what it is today: a globally unique specialist authority.

A look into the future shows: we cannot rest on the laurels of what we have achieved. The high dynamics in the development of information technology does not allow modern leading economies to stand still when it comes to digitalisation and IT security. We have to continue advancing our legal, technical and personal opportunities to shape digitalisation and to maintain and achieve IT security in the future.

During these strenuous times, the BSI's report on IT security in Germany in 2017 deserves particular attention. It is more than a snapshot. It is a profound and reliable documentation of which threats Germany's IT is exposed to and which challenges we have to face.

When reading the BSI report, the following becomes clear: BSI employees put a lot of effort into an area that affects millions of people, the problems of which are often only perceived by a few experts. They are the ones who perform the important tasks of prevention and detection of cyberattacks. They are the ones who find solutions for the most urgent challenges.

These challenging tasks make the BSI a supporting pillar of our digital Germany.

Berlin, August 2017

Dr. Thomas de Maizière, MdB
Federal Minister of the Interior

Foreword

Powerful and secure communication systems are the central nervous system of society in the 21st century. They are essential for a functioning economy and provide comfort and a wide range of opportunities in the private sphere as well. They create the preconditions for mobility and data exchange as well as for transfers of capital, goods and services. They are a prerequisite for Industry 4.0, the energy revolution and operation of critical infrastructures.

In the last few months, global attacks such as WannaCry and Petya / NotPetya as well as successful targeted cyber attacks on companies, on democratic institutions such as the German Bundestag and the parties, on decision-makers in business and not least on citizens made very clear how vulnerable our digitised economy and society is. The damage that is caused for companies and the general public has risen into the millions. With each incident, it becomes clearer how dependent successful digitalisation is on cyber security. The task and goal of the BSI as the national cyber security authority is to shape information security in digitalisation through prevention, detection and reaction for government, business and society.

As a competence centre for cyber security, the BSI enjoys a high reputation at all levels of society. In the BSI, all topics of cyber security are combined: from the protection of government networks and critical infrastructures through cryptography, certification and standardisation, consultancy for the Federal Administration, Federal States, business and society to shaping of digitalisation in highly complex projects such as energy transformation and autonomous driving. This bundling and networking of cyber security expertise in one authority gives the BSI its unique impact in Germany.

The report on the state of IT security in Germany describes and analyses the current IT security situation, also by presenting concrete examples and incidents. Based on this, we present the BSI's portfolio and solutions for improving IT security in Germany.

The first chapter deals equally with the threat facing the Federal Administration, the economy – especially critical infrastructures – and society. We describe the causes of cyber attacks and analyse the attacks and methods used.

We also show how the degree of dependency increases with the increasing networking of information and communication technology. We are all increasingly reliant on secure information routes, but at the same time the number of attacks on the network is growing. Cyber crime, cyber espionage and cyber sabotage of critical infrastructures represent serious threats.

Based on this, the second chapter of the Status Report deals with solutions to improve IT security in Germany and, above all, presents the offerings and activities of the BSI. Many examples show how the BSI works together with various stakeholders from the Federal Administration, the business world and society to mitigate the risks with effective and implementable security measures. Finally, the third chapter assesses the security situation, draws up recommendations and offers a forecast on further developments.

Experience shows that progress towards increasing cyber security is usually done step-by-step in the face of the reported threat situation. Yet the broader the awareness of the importance of information security in digitalisation for all sectors of society, the bigger these steps can be. That is what we are working on.

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

Contents

1 The Threat Situation

1 The Threat Situation

The following chapter describes the threat situation of IT security in Germany in 2016 / 17, divided into three areas: the Federal Administration, critical infrastructures / the business world and society. In addition, the attackers' methods and means are discussed, and a number of examples of how these attacks can affect or endanger public life in a digitised society are outlined.

1.1 The Threat Situation of the Federal Administration

The exercise of the constitutionally guaranteed tasks of the judiciary, legislative and executive powers requires secure and reliable operation of the Federal Administration's information systems. Only in this way is communication protected against manipulation of all kinds and a documentation of administrative action guaranteed. The confidence of citizens and corporations in the integrity of the digital state is shaken if they can no longer fulfil their tasks due to inoperative information systems. The information systems in government powers have thus become critical infrastructures for the community.

Insights from the Protection of Government Networks

Defence against attacks on Federal Administration IT systems is a core task of the BSI. In particular, the BSI has been responsible since the time of its founding to protect the Federal Government networks and today bears the overall responsibility for the IT security concept of the government network.

The key security measures for the central government network are consistently encrypted communication and a robust redundant architecture. In addition to this, regulated and trustworthy operation is ensured. Improvements to the security setup of the networks are implemented on an ongoing basis, and the networks of the Federal States and municipalities are closely connected.

The BSI has established a multi-level security system for the best possible protection of networks and IT systems. Apart from commercial protection products, it also consists of individually adapted and developed measures. They are continuously monitored, further developed and adapted to the dynamic threat situation. By combining different defence measures, the BSI can assess the IT security situation of government networks properly.

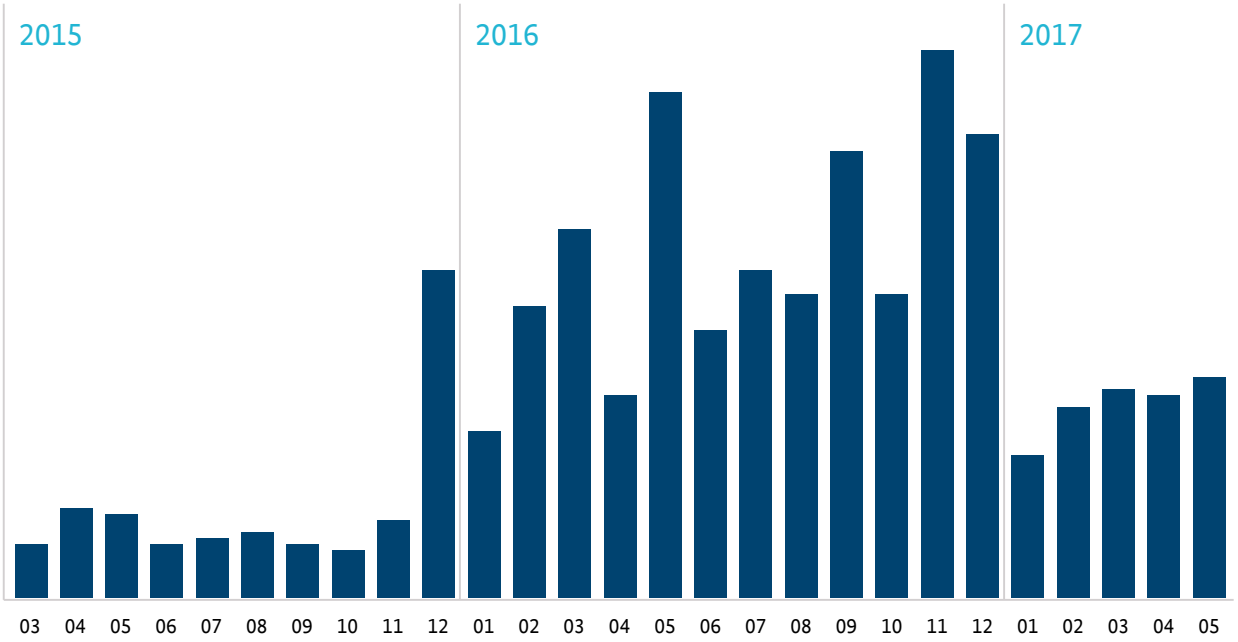


Figure 1 Automatically filtered malware at the network gateway of government networks through anti-virus protection measures

Defence against Malware

Cyber attacks on government networks take place every day. In addition to untargeted mass attacks, government networks are also exposed to targeted attack campaigns.

In this case, e-mails with malware are among the most frequently counted attacks on the Federal Administration. By means of automated anti-virus protection measures, an average of almost 52,000 such e-mails were intercepted in real-time per month before they reached the mailboxes of recipients. Of these, an average of around 11,000 malicious e-mails were collected each month only on the basis of non-commercial anti-virus signatures. The increase in these figures by 18 percent compared to the previous year is mainly due to the massive spread of ransomware in 2016, which could also be observed outside the government network. Attackers frequently used e-mail attachments with archived JavaScript or macro code in office documents in order to then download the actual malicious program from the Internet. Since the beginning of the year, the situation has noticeably eased. In the first half of 2017, only half as many e-mails with malware were intercepted as in the second half of 2016 – without any noticeable losses in the protection effect. Following the automated anti-virus protection measures, the BSI operates its own system for the detection of malware, which provides additional protection for the Federal Administration.

Staggered Defence

The various protection measures on the internet connections and on the client systems cannot always reliably repel all attempted attacks. For this reason, further measures for detection and reaction are implemented in the government network, which in such cases attack, prevent these attacks or minimize their negative effects.

For example, in the government network, outgoing network connections attemps are blocked on websites that distribute malicious programs. Likewise, attempts by already active malicious programs to connect with control servers that are used for control and data flow are prevented. In this way, already infected systems can be detected and unauthorised data flow can be prevented. Ideally, however, the attack is normally already prevented in advance, by preventing linking to malicious program distribution or a website used for phishing, for instance.

Using this method, around 5,100 attempts to connect to malicious code servers were prevented daily. These include long-running watering-hole attacks where perpetrators with an espionage background placed malicious code on websites relevant to government staff. The malicious code is exchanged at intervals of several months by new variants.

In less than 70 cases, Federal Authorities had to be informed about a potentional infection due to conspicuous behavior of one of their systems. This low number of potential infections is also due to the close-knit e-mail filters set up in response to ransomware campaigns, such as Locky.

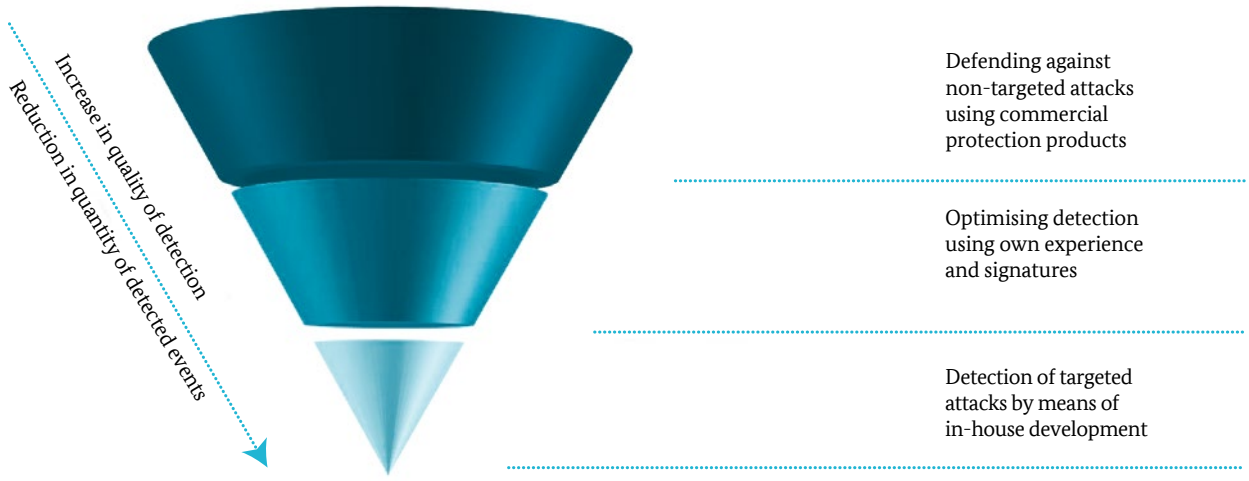


Figure 2 Tiered protective measures in government networks against email-based attacks

Findings from Information Security Consulting

The change in work processes by means of digitalisation also changes the requirements for the protection of the information processed there. Security measures must be constantly adapted to these changed conditions within the framework of the established management system for information security (ISMS), since the rapidly advancing digitalisation of the authorities' structures also allows an attacker to take advantage. In addition, there are new challenges to the ISMS of authorities posed by the Internet of Things, Industry 4.0 and the digitalisation of technical environments. If IP-based embedded systems, such as smart air-conditioning systems, are to be connected with government networks, this creates new potential risks for the information security that have to be dealt with appropriate measures.

The establishment of central IT service providers in the area of the Federal Administration as well as the increased use of the central government network presents the ISMS in the authorities with additional challenges that must be addressed parallel to regular operation and digitalisation.

- On the one hand, the authorities must consolidate their existing heterogeneous network structures and data centres to a common standard and adapt them to the new circumstances.
- On the other hand, information security must be ensured in all steps of consolidation and adaptation.

Another increasingly important aspect is that employees are interested in processes and solutions that they know from and appreciate in the consumer sector. The realisation of such solutions leads to various requirements for ISMS. As a result, authorities are being asked to make information security requirements more consistent with usability requirements and to make them more acceptable for security measures. In addition, the training and further education of IT security experts for authorities must be constantly advanced and expanded in order to be able to meet the attackers in this environment on equal footing.

Findings Based on Notifications from the Federal Administration

Pursuant to section 4 paragraph 3 of the Act on the Federal Office for Information Security (BSIG), Federal authorities are obliged to inform the BSI immediately of any successful or attempted attacks that are relevant to the protection against IT security risks, in particular with other authorities.

This mainly serves to conduct consolidated long-term analysis of the IT security situation. The question of whether and to what extent existing centralized protection measures are effective and economical is examined here. It is also determined whether there is a need for extended protective measures.

Although these reports are distributed irregularly over the years due to the very different threat situation, they nevertheless provide an additional indicator of the threat situation.

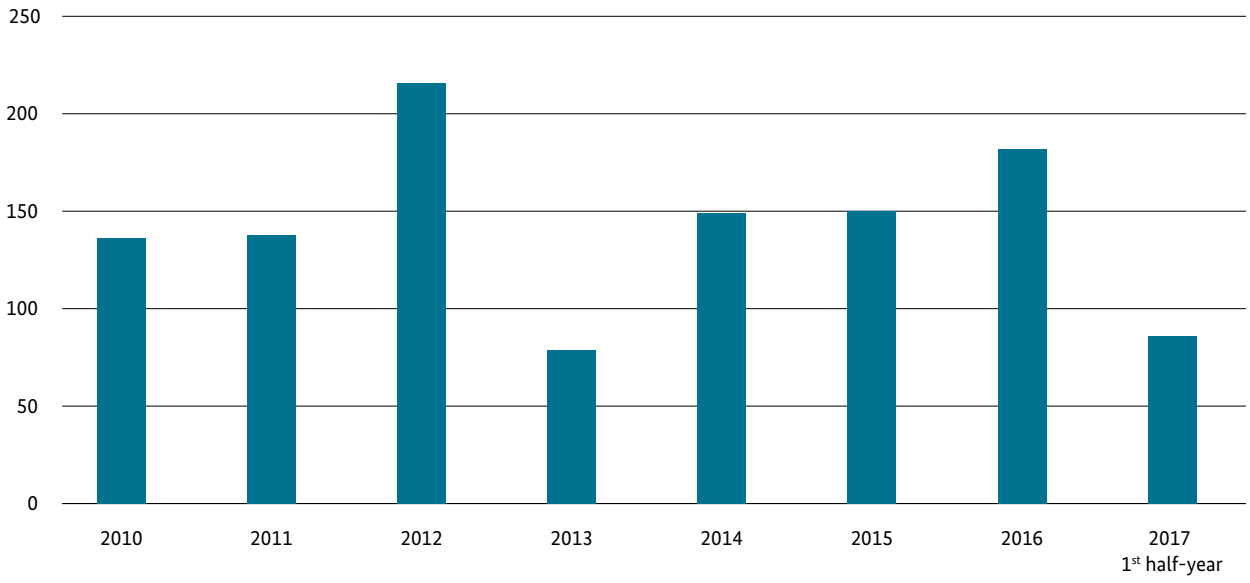


Figure 3 Number of obligatory notifications pursuant to section 4 paragraph 3 (BSIG)

In 2017, ransomware remained the authoritative source for malware infections. Attacks on telephone and video conferencing systems have also been reported.

1.2 The Threat Situation in the Business World

Critical infrastructures (KRITIS) are organisations and institutions of great importance to the community. Their systems and services such as the supply of water or heat, their infrastructure and logistics are increasingly dependent on a smoothly functioning information technology. A disruption, impairment or even a failure due to a cyber attack or IT security incident can lead to sustained shortages, significant disruption to public security and other dramatic consequences.

Findings from Reports under the IT Security Act

The IT Security Act entered into force in July 2015. At the same time, reporting requirements for operators of critical infrastructure were also introduced in a phased manner. They exist

- since the entry into force of the law for KRITIS operators obliged according to the Atomic Energy Act, the Energy Industry Act or the Telecommunications Act
- since the entry into force of the BSI KRITIS ordinance (03/05/2016) for KRITIS operators in the sectors of energy, food, information technology and telecommunications as well as water
- with the entry into force of the second part of the BSI KRITIS ordinance (30/06/2017) for KRITIS operators from the financial and insurance, health, transport and traffic sectors.

Since the introduction of the reporting requirement, 34 reports have been received by the BSI by 30 June 2017. Of these, 18 are in the information technology and telecommunications sector, eleven in the energy sector, three in the water sector and two in the food sector.

Due to the messages received, it can be determined that human errors such as incorrect configurations often lead to an IT malfunction. Hardware defects or faulty software are other common causes. The latter usually took the form of faulty updates. Depending on the design of the operator's infrastructure, these defects and faults had a partial impact on the availability of the critical infrastructure

Threat Differentiation by Industry

The high IT penetration in critical infrastructures is associated with high dependency on IT. As a result, not only the IT systems themselves are exposed to cyber security threats, but also the critical services involved. These damage potentials multiply. Critical infrastructures are thus at a particularly high risk, with initially the same threat situation as for other companies.

In addition, IT systems are used to provide services in the KRITIS sectors that are not comparable to conventional office or data centre IT. For example, many special systems and industrial control systems are used in the KRITIS sectors "Transport and Traffic," "Food," "Water" and "Energy." These systems usually require special treatment to protect against cyber threats, which must meet operational requirements for availability and reliability at the same time. Systems that are widely used and accessible over the Internet play an important role in the provision of critical services and are of particular importance due to the high damage potentials. The repeatedly successful cyber attack on the power grid in the Ukraine is a clear example of this. In December 2015, for example, at least

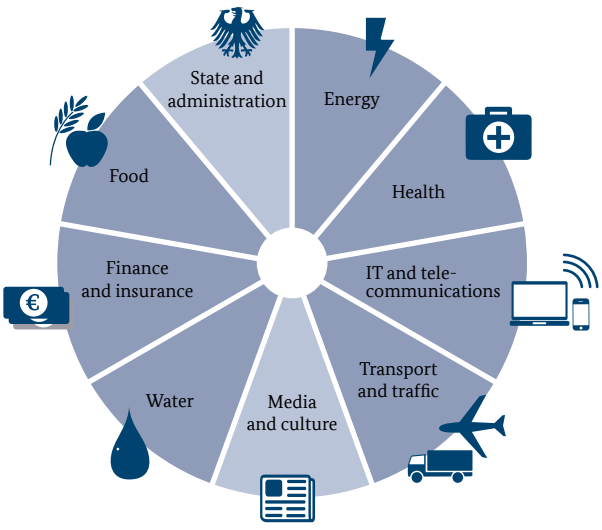


Figure 4 Seven of the nine KRITIS sectors come under the KRITIS revisions of the IT Security Act [1]

[1] The Federal Government has no regulatory authority for the media and culture KRITIS sector. The same applies to regional and municipal authorities in the state and administration sector. For the Federal Authorities included in the state and administration sector, comparable obligations to the current new regulations have already existed since the 2009 BSIG amendment.

225,000 people in the Ukraine were affected by a power failure caused by a targeted cyber attack that lasted for several hours. In December 2016, there was another power failure in Kiev, the capital of the Ukraine. According to the Managing Director of the state power utility Ukrenergo, this was yet another targeted cyber attack. Between 100,000 and 200,000 inhabitants were without electricity for over an hour.

The failure of Deutsche Telekom routers in November 2016, in which a cyber attack disrupted Internet access at approx. 900,000 customer lines throughout Germany, also clearly demonstrated the risk potential of a cyber attack on the telecommunications infrastructure (see info box on page 15).

The vulnerabilities detected in the remote access software of construction site traffic lights, which are accessible via the Internet (see infobox on page 14), are another example of this. In this particular case, no damage was caused. The safeguarding of special systems has its own problems, which in this case only caused increased exposure.

Critical infrastructure operators are still the focus of attackers with a political motivation, e.g. hacktivists, state-sponsored actors or terrorists. Because a successful attack would publicly have an impact on the economy or the daily life of the population, critical infrastructures remain a worthwhile target for these groups of attackers. This is especially true for politically motivated attackers who want to put their own political agenda at the centre of public attention through an attack.

Other Findings on the Threat Situation for Companies

Companies in Germany are interesting targets for cyber-espionage due to their technological know-how and their international activities. Over the last few years, many companies have responded and established their own computer emergency teams (CERTs) as well as intersectoral information exchange organisations.

Companies are principally exposed to the same risks as any other IT and Internet user. In addition, they are exposed to attacks that do not occur in the private sphere. These include CEO fraud (see chapter 2), for example, where employees of companies are instructed to transfer large sums of money to accounts that are subject to the control of the attackers. In the case of ransomware attacks, one can observe that higher ransom is demanded from companies than from private users.

Following a worldwide trend, the number of observed cyber-espionage attacks against businesses declined sharply in Germany as well at the end of 2015 and in early 2016. In the meantime, the number of attacks observed has risen again. Since the summer of 2016, new attacks on German companies are being seen again. Particularly high media interest was shown in the attack with the malicious software Winnti on a German industrial company (see infobox on page 12). The BSI is also aware of further attacks on German companies involving Winnti.

APT groups also carried out espionage attacks on German companies. It is worth noting that the groups APT28 and APT29 hardly appeared in attacks on German companies. Apart from armaments companies, these groups seem to focus primarily on government institutions and political organisations. Not least due to the extensive international activities and international interweaving of German companies, the BSI has analysed public reports on which cyber espionage groups are active in various industries around the world. Besides government institutions and the opposition in non-democratic states, the areas of armaments, energy and media are those with the most active groups of perpetrators (see figure on page 13).

Criminals also increasingly use techniques known to date only from espionage attacks. For example, the Lazarus Group attacked banks around the world to initiate bogus payment transfers via the SWIFT network. The Carbanak Group, in turn, compromised financial institutions and ATMs to also falsify payment transfers. Both groups employed techniques that go beyond the methods

Cyber Attack on a German Industrial Company

Situation

At a German industrial company, data leakages through a cyber attack occurred in mid-2016. According to the company, it was an attack group from the Southeast Asian region. This assessment is shared by the BSI, however, it is unclear whether there is actually only one hacker group behind the attack. The perpetrators gained access to the internal network and then spread worldwide through different sites. The incident was detected approximately two months after the initial infection, when massive failed logins were observed on systems. This circumstance is an indication that the perpetrators used access data that they captured on compromised systems to spread to other systems. They also had the ability usual for APT groups to spread in an enterprise network unnoticed over an extended period of time.

Cause and Damage

According to public reports, the attack was carried out by the Winnti malware, which is used by Asian perpetrators and uses sophisticated techniques to camouflage traffic to the perpetrators' control servers. The addresses of the control servers are stored dynamically on legitimate websites, which are designed to be edited by users. Since these legitimate websites are typically addressed in TLS / SSL encrypted form, it is hardly possible for network defendants to identify malicious software traffic without a doubt. Winnti is a comparatively advanced software that is comfortable for the perpetrators. As a rule, it is observed together with the malicious software PlugX, frequently used in Asia, which gives the perpetrators full control over an infected computer. The perpetrators behind Winnti originated in the development of criminal fake anti-virus malware and then switched to financially motivated attacks on game companies. The exact attack vector was either not found or at least not reported to the public. This form of attack is done in general by spear phishing e-mails that contain attachments with malicious code or links to malicious websites. In rare cases, the initial compromise is achieved via servers that are no longer maintained and accessible from the Internet, from which the perpetrators spread to the internal network in the case of suboptimal network architectures. Data was affected which could have given the perpetrators or their customers a technological advantage. The industrial company confirmed that technological data were stolen. According to the company it is however unclear whether by the data outflow had arisen a damage, for example, on intellectual property.

Reaction

The correction of the large area infection took the company CERT several months with the help of external specialists. The company also decided to have the experts accompanied by a journalist. After the completion of the adjustment measures, he was able to report the incident in several articles. The company even received positive feedback from the security community.

Recommendation

Potential targets of APT groups are in principle all companies that are active on the world market or occupy top technological positions. The aim of the perpetrators is to achieve technological or market-operative information. The incident shows that the security level of international locations must be aligned with the standard of the main location as these sites are integrated into the enterprise network. Alternatively, a clear separation of the networks and domains can be maintained. The infection of a system should not cause to compromise entire network areas or central servers. In addition, continuous network monitoring is irreplaceable to quickly detect compromises.

observed with normal crime ware. This includes tailored social engineering on selected employees and the lateral movement, i.e. the spreading in the internal network by using stolen access data and extending user rights.

Cyber-espionage continues to be a challenge against which companies need to arm themselves. Since the initial attacks are often based on the less secure networks of foreign locations or acquired subsidiaries, the focus should be on achieving a uniform IT security level across the enterprise. Since the IT networks are not sufficiently separated in many companies, the attackers are otherwise able to permeate the company network globally too easily. If standard security measures have been established across the company, network monitoring processes should subsequently be developed and implemented. If these infrastructures and trained personnel exist, one can also consider the purchase of Threat Intelligence.

Government institutions	APT6/1.php, APT12/NumberedP., APT28/Sofacy, APT29/CozyBear, APT32/OceanLotus, Cadelle/Chafer, Callisto/DancingSal., CharmingKitten, Danti, DarkHotel, Dropping-Elephant, EmissaryPanda, Gamaredon, GazaCybergang, GothicPanda, Greenbug, Groundbait, HammerPanda, Infy, KeyBoy, Longhorn, LotusPanda, Machete, Mofang, Naikon/OverrideP., NanHaiShu, OilRig, Operation-Cleaver, Remsec/ProjectSauron, ScarletMimic, Shamoon, Snake, Suckfly, TidePool/Ke3chang, Transparent-Tribe, TropicTrooper/PirateP., ViceroyTiger
Military / Defence	APT28/Sofacy, AridViper, Callisto/DancingSal., CharmingKitten, C-Major/PureStrike, Dropping-Elephant, Gamaredon, GazaCybergang, GothicPanda, HammerPanda, LotusPanda, Machete, Mofang, Naikon/OverrideP., OilRig, Operation-Cleaver, Remsec/ProjectSauron, Snake
Energy	APT10, APT18/Wekby, APT29/CozyBear, CharmingKitten, ElectricPowder, EmissaryPanda, Greenbug, Kraken/Laziok, Longhorn, Machete, OnionDog, OperationCleaver, Sandworm, Shamoon, TropicTrooper/PirateP.
Opposition	Ahtapot, APT32/OceanLotus, Bookworm, FlyingDragon, Groundbait, Group5, Infy, Neodymium, Operation-Cleaver, Operation Manul, Promethium, ScarletMimic, Sima, StealthFalcon
Media	APT28/Sofacy, APT32/OceanLotus, BugDrop, Callisto/DancingSal., DarkHotel, GazaCybergang, Groundbait, Infy, Operation Manul, Sandworm, ShroudedCrossbow, StealthFalcon, Tick
Finance	APT18/Wekby, APT29/CozyBear, EmissaryPanda, EquationGroup, GazaCybergang, HammerPanda, Longhorn, OilRig, Sandworm, Suckfly
Telco	APT18/Wekby, Codoso, EmissaryPanda, HammerPanda, Longhorn, Machete, OilRig, Remsec/ProjectSauron
NGO	APT29/CozyBear, Callisto/DancingSal., CharmingKitten, HammerPanda, Infy, NilePhish, Operation-Cleaver, RocketKitten
University	APT10/menuPass, BugDrop, Codoso, Greenbug, DarkHotel, Longhorn, RocketKitten
High-Tech	APT18/Wekby, CharmingKitten, Codoso, LEAD/Winnti, Tick
Transport / Logistics	Cadelle/Chafer, OilRig, OnionDog, Remsec/ProjectSauron, Shamoon
Aerospace	APT28, EmissaryPanda, HammerPanda, Greenbug, Longhorn
Health	APT10/menuPass, LEAD/Winnti, Suckfly
Law office	APT29/CozyBear, Codoso, DeepPanda, NanHaiShu

Figure 5 List of the cyber espionage groups active worldwide in various industries during the period under review

Cyber Security by Design: Manipulatable Construction Site Traffic Lights & Waterworks

Situation
In August 2016, the BSI learned of the possible abuse of a known vulnerability in software that can be used among others in construction site traffic lights. The traffic lights in question are directly accessible from the Internet and potentially manipulated. In addition, the BSI has been made aware of several open, web-based control systems from waterworks in Germany.

Cause and Damage
For the traffic lights, an obsolete remote maintenance software (RealVNC) is used that has known weak points, allowing unauthorised access. Updates for these vulnerabilities are available but have not been installed. In some of the reported light signalling systems, the BSI was reported that the authorised use was logged off, allowing direct access to the system. An automatic logout function was apparently not available. A takeover and control of the traffic lights would therefore be fundamentally conceivable, which could lead to a dangerous interference with road traffic. In waterworks, Human Machine Interfaces (HMI), i.e. user interfaces, were used. At least one read access from the Internet was possible. Further accesses leading to outside control cannot be ruled out.

Reaction
In the present case, the BSI could not confirm the described constellation of a potential remote control of the installations. The BSI, however, is considering a possible misuse of the signal control of construction sites as a matter of principle.

The operators of the waterworks were contacted directly by the BSI and shown the situation. They were unaware of this accessibility of the systems from the Internet. They reacted very cooperatively and closed the open accesses in the short term. In the case of a subsequent inspection carried out by the BSI, the installations were no longer publicly available.

Recommendation
Producers of construction site traffic lights and other systems connected via the Internet are required to give the IT security of their products at least the same importance as the ergonomics or the price. In the sense of a “security-by-design” approach, IT security should be considered and implemented even during product development. In support of secure development, the BSI has formulated questions in the “ICS Security Compendium – Testing and Requirements for Component Manufacturers” to help manufacturers test their components and avoid vulnerabilities. The document is available on the BSI website.

Operators of critical infrastructures using HMI should check which of the controllers are vulnerable in principle. Above all, in the case of control systems with Internet access (e.g. remote maintenance), they should consider whether remote access is imperative and, if so, how the control systems are visible from the Internet? For remote access, safety measures such as VPN should be established and it should be checked whether the planned IT security measures (target / actual comparison) are taking effect. In addition, operators should note the recommendations of the BSI ICS Security Compendium, which is also available on the BSI website.

The IT security of connected systems will increasingly become a quality feature in the future. The Federal Government’s cyber security strategy provides for the development of a corresponding quality seal, which is currently being developed by the BSI. Manufacturers can express the IT security-related quality of a product already by referring to its certification.

Crashed Telekom Routers

Situation

On Sunday, 27 November 2016, there were disruptions of connections for Deutsche Telekom concerning, among other things, general Internet access as well as VoIP and IPTV services. About 900,000 customer connections were affected by this disturbance Germany-wide. The Telekom routers were immune to the attempt of the infection by a vulnerability found in routers of the manufacturer Zyxel. However, they reacted incorrectly due to another, previously unknown vulnerability. This led to the massive disturbances.

Cause and Damage

The cause of the impairments was a worldwide cyber attack with the aim of infecting Internet routers with malicious code and making them part of a botnet. The malicious software used was an advanced development of the bot software Mirai. The cyber criminals used, among other things, a vulnerability found in routers of the manufacturer Zyxel in the implementation of protocol TR-064. This is usually used for simple router configuration by customers. The discovered vulnerability became critical because the protocol could also be wrongly addressed from the Internet. The port 7547 was used for this router model. It is actually assigned to protocol TR-069, which is used by some Internet service providers to administrate routers remotely or to automatically update them. In this case, the attacker took advantage of this by indiscriminately contacting any router found on the Internet with the attack vectors implemented previously in Mirai on port 7547. The aim was to infect the device and take control.

Reaction

A short-term solution to the problem could be achieved by restarting the router, but the attacks were so numerous that the routers crashed again in just a few minutes. In cooperation with the device manufacturer, Telekom ultimately offered a solution by providing a fast update, so that the situation normalised within a few days.

Recommendation

Due to the incidents at Telekom, the remote configuration service according to TR-069 and the release of the corresponding port 7547 beyond the Telekom network were particularly criticised. With appropriately secure implementation and configuration, TR-069 is now considered safe for home network routers. The update for the routers was also automatically implemented via TR-069. This meant that the effort for the affected customers could be kept small. The criticism of the accessibility of the routers via the port provided for TR-069 from the Internet can only be considered as partially justified. A net side barrier for Telekom could have prevented the collateral damages in the form of failures. If, however, the port standardised for TR-069 is blocked, third-party providers of home network routers can no longer provide firmware updates and other support services to their customers. One possibility would be to restrict access to the remote maintenance function of the routers through so-called access control lists (ACL located on the routers themselves).

1.3 The Threat Situation in Society

Networking and digitalisation have an increasing impact on society and the everyday life of our citizens. IT solutions are an obvious factor in many social spheres of life. A life without the Internet is hardly imaginable in today's society because millions of people use mobile devices such as smartphones and tablets.

The high degree of penetration of IT in all areas of social life is associated with many opportunities, but also entails risks in the areas of security and data protection. The issue of cyber security in the sense of comprehensive IT security precautions and improved ability to act in the event of a cyber attack is the prerequisite for successful digitalisation.

Threats Related to the Internet of Things

In the context of increasing digitalisation, the Internet of Things (IoT) is increasingly moving into the homes and the personal sphere of users. More and more networked devices are enabling new applications to increase comfort, for example in the area of household appliance control, home surveillance or health management. At the same time, previously existing hurdles for the end-user are eliminated, as radio-based solutions or powerline technologies replace the cabling that was needed before. This leads to an ever higher networking density.

Nevertheless, IT security previously played a marginal role or no role at all with IoT devices. The functionality of a device and the associated comfort as well as the price are usually the main factors in a customer's decision to purchase a device. This creates a new area of threat, a larger area of attack that cyber criminals can use for their purposes.

The attacks on IoT devices are generally carried out directly over the Internet or "over-the-air" via existing radio interfaces. There are different threat situations with different types of threats:

- The IoT device is attacked to cause direct damage to the user. For example, smart home components for access control are attacked and manipulated to prepare a burglary. Here, a compromised webcam can provide confidential information about the residents and their behaviour.

- The IoT device is compromised and used to attack other infrastructure components or services. Frequently, unsecured or insufficiently secured IoT devices are compromised and merged into botnets in order to carry out targeted DDoS attacks against websites or web services from third parties. In this case, the attack often remains undetected for the user since he is not directly affected by its effects. This approach can be observed, for example, in the Mirai botnet.

- The IoT device is disabled by a malicious program and is, at least temporarily, unavailable to the end user. Small and medium-sized enterprises (SMEs) have been affected recently and their infrastructure was no longer accessible for days on the Internet.

The possible effects of the aforementioned cyber attacks are manifold. Besides direct attacks on privacy, personal data, access information, and end-user assets, the abuse of IoT devices leads to massive economic damage by DDoS attacks on major (critical) infrastructure components and services.

Threats from Mobile Communication

Smartphones and tablets have become indispensable for many of us. They enrich communication and entertainment and enable navigation and interaction via social networks. Application programs that are installed in a few simple steps – apps – make this possible. The increasingly intensive use of apps also ensures that more and more sensitive data is processed on the devices. Address books, location and access data, e-mails and other communications data make mobile devices an increasingly attractive target for criminals. Their safety is influenced by many aspects:

- Users often grant privacy and security often little importance or at most a subordinate role in app selection. The combination of usefulness and convenience as well as the cost are crucial for choosing an app. But the possible outflow of personal or critical data constitutes a loss of control associated with potentially significant dangers.

- The installation of software updates to eliminate gaps is a prerequisite for the secure operation of mobile devices. However, due to the variety of device types, both on the hardware and software level, a short-term and comprehensive supply of updates by manufacturers and suppliers isn't an easy task. Despite industry initiatives aimed at accelerating this, many mobile devices, especially with the Android operating system, were on a security-critical software stand during the current reporting period.

- Some of the personal and sensitive information on mobile devices is not or only insufficiently encrypted and often stored in a cloud. The user thus entrusts his data to the cloud vendor. If access is not sufficiently protected, both the user's data and the access data for the cloud itself can fall into the wrong hands.

- Mobile devices often connect to public hotspots. Here, the data is usually transmitted in an unencrypted manner and can therefore be read by unauthorised third parties. Unique user identifications such as the International Mobile Subscriber Identification (IMSI) are potentially affected.

- Operators of mobile networks as well as app providers are able to locate mobile devices and thus also determine the location of the owner. Vulnerabilities in the mobile operator's infrastructure can lead to the location of mobile devices being also possible by third parties. Attackers can thus create a comprehensive geolocation profile of the victim.

- Calls over second-generation mobile radio technology (2G / GSM) can still be monitored on the radio interface. This also affects 3G and 4G wireless technology, since the attacker can in many cases provoke a switch to the 2G standard. User identifications such as the IMSI can also be accessed on the radio interface.

- The increasing use of SMS as an authentication factor and the authorisation of transactions (mTAN procedure) also incurs risks. An attacker can redirect the SMS traffic by exploiting vulnerabilities in the network infrastructure, thus misusing the codes sent. In the reporting period, there were vulnerabilities in the SS7 protocol, for example, which is important for the exchange between mobile networks, and thus the possibility of intercepting SMS messages during online banking. Such abuse is also possible by malicious software finding its way onto the device.

The impact of these numerous vulnerabilities on the protection of privacy and sensitive data is as impressive as it is manifold. Through the outflow of personal data, be it through apps on the device, the network operator or cloud vendor, detailed conclusions can be drawn on the behaviour, interests, places of stay and mindset of the user. This information could subsequently be used for advertising purposes without the consent of the respective individual, or be stored for an indefinite period, for criminal purposes or for the discrediting of a person.

On the other hand, the mobile devices themselves are the target of active attacks. If security updates have not been performed, an attacker can also take control of the mobile device, as with stationary computers. In addition to the usual misuse of resources (e.g. integration into a botnet), the monetary risk of malicious software in the mobile context is very high, since it is possible to run up costly telephone calls, SMS messages or other premium services without the person concerned even being involved.

Findings from Attacks on Public Institutions and Functionaries

The influence of political opinion-making in elections has been the focus of public discussion especially in the context of the presidential elections in the US and France as well as the election in the Netherlands. In Germany there is also the possibility that perpetrators could attempt to influence the 2017 Bundestag election digitally.

Fake news is spreading rapidly in the social networks and is sometimes accepted by established media unchecked. Social bots (automated programs that pretend to be people with real identities) gather information about users (e.g. from Facebook), spread specific messages (e.g. through tweets on Twitter) and participate in discussions to suggest majority opinions and to generate reports on hot topics.

In addition, social bots are able to send individualised messages to specific target audiences in which potential victims (for example, members of an organisation's electoral team) are tempted to access links to malicious websites. If a user follows these links, there is the risk that malicious software will be installed on his computer. In the next step, confidential data can be collected that is used by the victim or the organisation. Further information technology attacks with the help of social bots are conceivable. For example, by means of massively generated comments, information pages for elections or candidates in social networks could be rendered illegible or unusable. In addition, identity theft or other forms of attack are conceivable.

Although the BSI has not received any concrete information about planned cyber attacks on the Bundestag election, Germany must be prepared for this scenario – also against the backdrop of the cyber attacks that have taken place in the US and France. Possible targets for cyber attacks in the context of elections are, in particular, parliaments, parliamentarians, authorities, parties (the media, journalists, Facebook, Twitter) as well as IT used at all Federal Levels.

1.4 Attack Methods and Means

Effective protection against cyber attacks is only possible if cyber threats and one's own vulnerabilities are at least generally understood. This knowledge is required for selecting suitable preventive and reactive measures against such threats and for creating a basis for risk analytics.

A key component of cyber security is the defence against attacks. Due to the dynamic development of the cyber security situation, this aspect has to be regularly targeted and re-evaluated, because attack methods and means are easily and cost-effectively available and obtainable. The latest findings on vulnerabilities and attacks are already being used for cyber attacks after only a short time. However, despite the large number of different attack targets and possible attack methods, trends and tendencies that can be used for successful defence can be identified.

1.4.1 Vulnerabilities in Software

As in recent years, there have been a large number of critical vulnerabilities in software products regularly evaluated by the BSI (see figure 6) in 2016 / 17. This trend generally applies to other software products which are not explicitly considered here.

Investigations such as the Coverity Scan Open Source Report show that the average number of errors per line of source code (defect density) has decreased slightly in recent years. This suggests an improvement in software development processes. In turn, however, the scope of the codebase of software products is also increasing, so that the existence of critical weaknesses can be assumed for any sufficiently complex software product – either as an integral part of a hardware product (e.g. heart pacemaker) or as an optional additional function of a combined hardware and software system (e.g. office package for a smartphone). Since only a part of the detected errors are removed or published, there is always a latent threat from vulnerabilities that are not publicly known and for which there are no security updates available yet. Therefore, it should be assumed that the software used always contains vulnerabilities that are also exploited ("assume breach" paradigm).

Vulnerability Lifecycle

If security updates are promptly implemented by the user, there is generally no risk of publicly known closed vulnerabilities. This applies to the majority of the vulnerabilities evaluated by the BSI. The Responsible Disclosure Strategy, according to which all parties involved

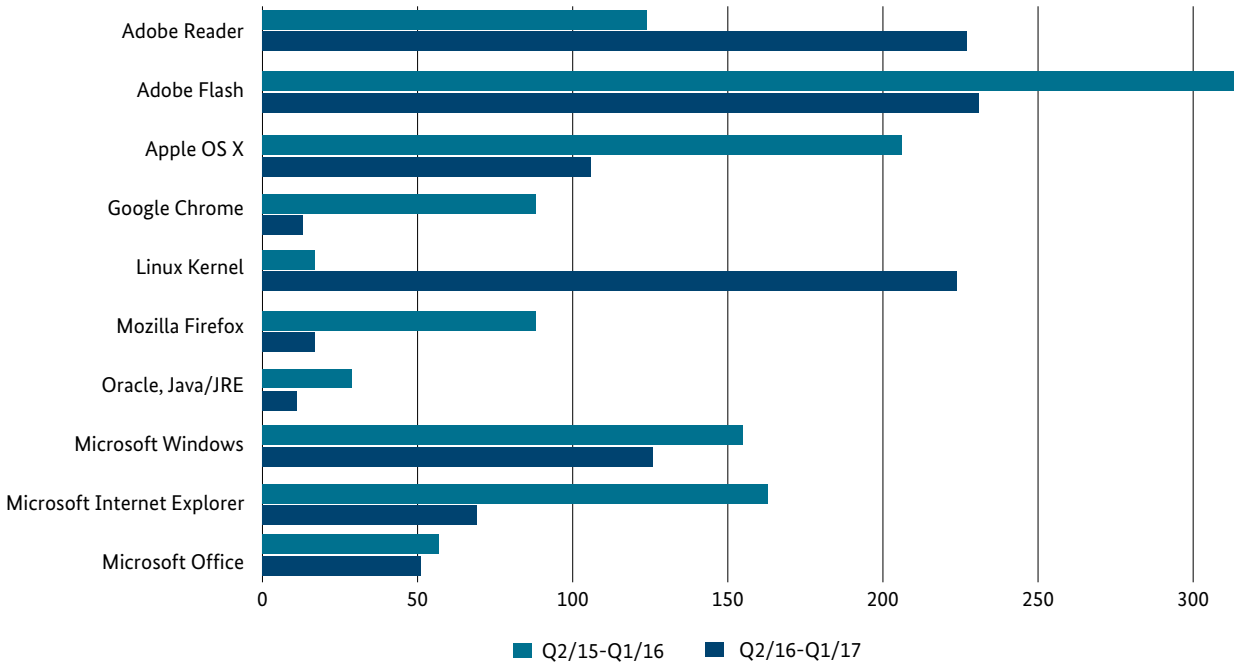


Figure 6 Solved critical vulnerabilities by product

Data Theft at Yahoo

Situation

In September 2016, the US Internet company Yahoo admitted that in late 2014 they had been the victim of a cyber attack in which the profile data from 500 million registered users was stolen. To date, this was probably the most comprehensive theft of user data worldwide. In addition to the names of the users, the stolen records also contained their e-mail addresses, telephone numbers, birth dates and password hashes. In December 2016, Yahoo finally announced that it had been the victim of a much larger data theft as early as August 2013. User data from one billion user accounts was stolen.

Cause and Damage

Yahoo encrypted passwords in two ways – via coding and using a technique called hashing. However, hackers are now able to crack secured passwords by creating huge encyclopaedias with similarly encrypted terms and matching them with databases of stolen passwords. In addition, the active utilisation of a vulnerability was known in the processing of so-called cookies. Cookies are small text fragments containing information about the current user that is stored in the browser. This allows a user to also later access Web applications after a single logon, without having to re-submit his access data. In the case of Yahoo, it was possible to fake these cookies. Thus, attackers could access Yahoo user accounts without knowing the current access data. The vulnerabilities have now been closed.

Reaction

In the interests of German users, the BSI has contacted Yahoo to obtain information on the details of the attack, the exact extent of the damage incurred and the measures taken. Yahoo! EMEA Ltd. in Dublin showed little cooperative support and did not support the BSI in the analysis of security incidents. The company refused to provide the BSI with any information, but instead forwarded it to the Irish Data Protection Commissioner, without, however, authorising it to provide information to the BSI. Due to the lack of cooperation, the BSI does not yet have any concrete information that could be used to deal with these incidents, and ultimately to provide advice and warn users to prevent more similar possible incidents. Nor has the BSI been able to ascertain whether the measures taken by Yahoo to ensure the security of its systems are appropriate and sufficient for users.

Recommendation

These incidents demonstrate the extent to which service providers can be compromised. It is also clear that it is imperative to establish a holistic security concept. An open and customer-friendly approach to security incidents should also be understood as part of corporate culture. In view of the large number of affected accounts, the BSI assumed that German users were also among the victims. It has advised users who have a Yahoo account or had one in the past to change the password for it, as well as the personal security questions and answers provided by Yahoo, and to no longer use it for other Internet services, online stores or social media accounts. In the face of repeated cases of data theft, however, users should also look more closely at the services they want to use in the future, while making security a decision criterion. An examination by the legislator as to whether the existing information obligations of the service providers are sufficient also seems to make sense.

Vulnerabilities at 1,000 Online Shops in Germany

Situation
Cyber criminals used vulnerabilities from the Magento e-commerce software to inject malicious program code into online shops. This pegged payment information and other personal data entered by customers when placing an order, and transmitted it to the perpetrators.

Cause and Damage
In numerous online shops were outdated versions of “Magento” in use. In September 2016, nearly 6,000 online shops affected by these “online skimming” attacks were identified worldwide, including several hundred shops operated in Germany. The vulnerabilities exploited by the attackers were however not closed by many shop owners despite existing software updates. This allowed the cyber criminals to check out data entered by customers with their orders. By January 2017, the number of known online stores affected in Germany rose to at least 1,000.

Reaction
In September 2016, the CERT-Bund notified the relevant network operators of online shops in Germany. Providers were asked to inform their affected customers (shop owners) accordingly. The imported code was not removed at many shops, or the shops were compromised again. Parallel to a renewed notification of German network operators, the BSI therefore published a press release in January 2017, in order to also publicly point out the facts, to raise awareness among shop operators and to call to action. Since June 2017, the Implementation Act for the NIS Directive has also expanded the providers‘ instruments, in which the authority to act has been significantly strengthened.

Recommendation
Users who are notified by their network operators or otherwise about software vulnerabilities in deployed products should immediately close them by running appropriate updates. Delays play into the hands of the cyber criminals, who can continue to exploit the vulnerabilities. Samples conducted in March 2017, showed that numerous shop operators responded to the provider’s and the BSI’s warnings and removed the malicious code and closed the vulnerabilities through an update.

How many Vulnerabilities does a Software have?

The number of publicly known vulnerabilities, as listed, for example, in the CVE database is always only a subset of all the vulnerabilities of a product. It does not allow any conclusions to be drawn about the number of non-public or still undiscovered vulnerabilities. Neither can clarity be deduced from this as to how new or published vulnerabilities will develop.

Therefore, there is also no basis for trend analytics or situation pictures, e.g. based on data from the CVE database. There is also no correlation between the nature of the vulnerability and the time that the weak spot remains undiscovered or unpublished. Finally, in the case of counting CVE numbers, several factors have to be considered, which make a comparison of numbers appear only to a limited extent:

- Some software vendors only assign a CVE number to publicly known vulnerabilities. As confidential reported or internally found vulnerabilities remain without a CVE number.
- Other software vendors aggregate multiple vulnerabilities into a single CVE number, unless one of the vulnerabilities already has its own CVE number.
- In addition, not all vulnerabilities are recognised as such and are potentially only classified as normal troubleshooting, whereby a CVE number does not initially appear to be necessary. In the later recognition of the safety relevance, a CVE number is sometimes assigned depending on the vendor.
- Changing of the counting philosophy of a vendor from time to time is not uncommon.
- In addition, the entries in the official CVE database can only be found with considerable time delays.

agree on a specific deadline within which a vulnerability is removed before any details are published, seems to work. More and more seldom, information about vulnerabilities is published where the vendor finds out at the same time as the public.

On the other hand, if there is information about a current vulnerability that is sufficiently detailed to be used by an attacker, it is a so-called zero-day vulnerability. Since a short period of time is expected until exploitation, they represent a direct threat to the general public. A recent study by RAND Corporation reveals an average time of 22 days between the public finding out about a vulnerability and the availability of an exploit, whereby the period can also be considerably shorter in individual cases. For this reason, the rapid provision of security updates by the vendor and their rapid installation by the user is so important.

A Responsible Disclosure Agreement (e.g. with a publication period of 90 days) is therefore advantageous for all three parties: The finder of a vulnerability avoids the risk of being made responsible for the exploitation of it, the software vendor can analyse and fix the error in a reasonable time, and the user can assume that the vendor cannot delay the availability of a patch for an unlimited period of time.

Bounty Programs of Limited Value

There are various approaches to reducing the number of open vulnerabilities in software products. Intensive security checks or the purchase of vulnerability information (so-called “bug bounty programs”) can lead to the detection of individual vulnerabilities, but they are not sufficient to obtain error-free products.

Since an attacker usually benefits from a single vulnerability in order to exploit it in a software product, but a vendor or defender has to eliminate all vulnerabilities, the search and removal of vulnerabilities is necessary, but not sufficient. It must be assumed that there are always vulnerabilities that can be exploited sooner or later (“assume breach”).

Therefore, further measures are necessary for appropriate protection, and speed and quality of the work must be weighed in their implementation. This includes, in the short term, single classes of exploits such as stack overflows or type interpretation errors. For example, stack overflows can either be prevented or at least their productive exploitation made impossible by appropriate measures of the programmer when creating programs. However, those strategic measures are more sustainable reducing the impact of the attack. Depending on the protection requirement, this includes, for example, a physical isolation or separation of critical systems.

An indispensable part of a measure catalogue is also adequate recording in conjunction with an evaluation designed to detect vulnerabilities exploitation. The safety limits built up by the separation serve not only to limit damage, but can also be used to detect attacks at an early stage.

1.4.2 Malware

The term malware is a catch-all of all types of computer programs that perform unwanted or malicious functions on a computer system. The distinction between trojans, viruses, worms, etc. is hardly relevant today, the terms are used mostly synonymously for all kinds of malware. The successful infection of systems with malware forms the basis for common business models of cyber crime such as ransomware or botnets, and is also used for other forms of cyber attacks, e.g. APT attacks. While around 350,000 new malware variants were still being viewed daily in 2016, a decline is currently apparent. From January to May 2017 about 280,000 new malware variants were observed per day. Overall, there is currently a significant reduction in the transmission of malware spam, following the massive spread of ransomware trojans in 2016.

Routes of Infection

The most common routes of infection for malware are e-mail attachments as well as the user's unnoticed infection when visiting websites, so-called drive-by downloads. Also, the direct download of malware via weblink is more frequently observed. Infections caused by the direct utilisation of other vulnerabilities, as in the case of the ransomware WannaCry, are comparatively rare. The attackers frequently used malicious code in the form of JavaScript files for infection. The malicious code in the form of macros embedded in Office documents is also widely used. In both cases, the actual malware is mostly downloaded from the Internet or generated locally after the embedded malicious code is executed.

Detecting Malware

Classic, signature-based AV products offer only a basic protection against malware infections, since new malware variants are generated faster than they can be analysed. Malware spam waves are often already terminated before new AV signatures can be created and imported.

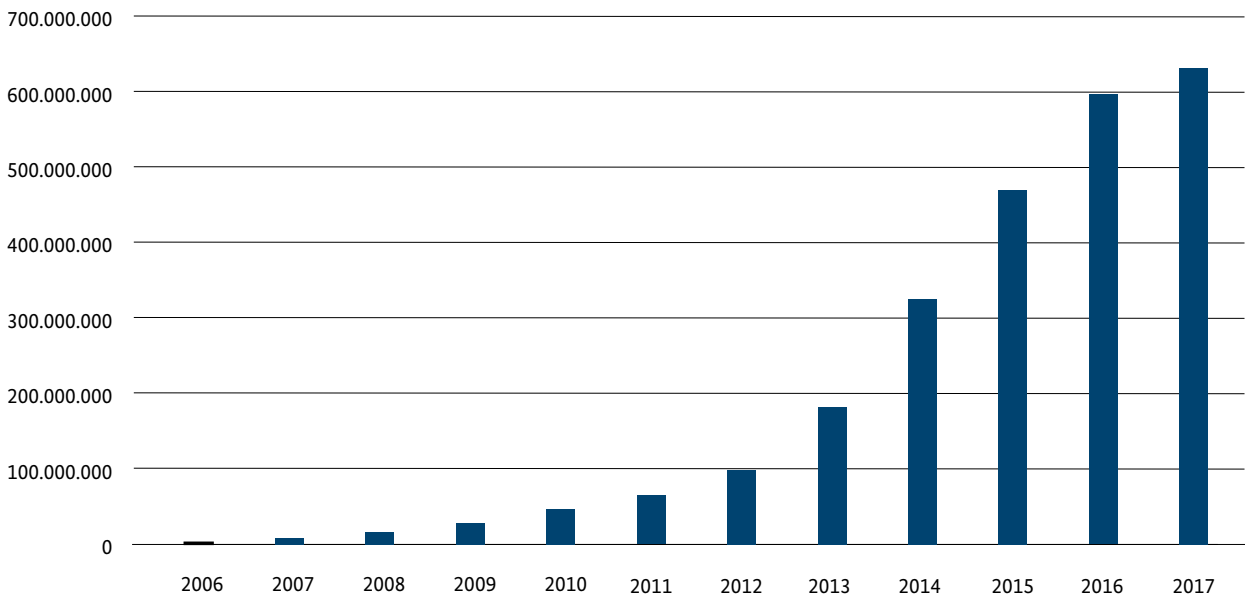


Figure 7 Known malware (2017 up to May), source AV-TEST GmbH

In addition, the analysis of malware is increasingly complicated by integrated functions, which are used to identify analysis tools and environments. In the meantime, macro viruses also use different techniques to determine whether they are executed in an analysis environment. In order to obscure the communication of a malware, compromised websites of third parties are abused as a control server and as a propagation path. For example, the good reputation of an existing, compromised website is exploited to circumvent potential URL filters.

Infections with malware, especially with ransomware, after untargeted attacks were named by companies as the most frequent type of attack in the cyber security survey 2016 by the Allianz für Cyber-Sicherheit.

Threat Situation Remains Critical

As in previous years, malware is one of the biggest threats to private users, businesses and authorities, even in the current reporting period. In spite of the decline in numbers, no all-clear signal can be given. Due to the advancing digitalisation and mobility, mobile and alternative platforms are also becoming more and more the focus of the attackers.

Through the ongoing technical development of malware, classic defence measures are increasingly losing their effectiveness. By partially very sophisticatedly designed social engineering, the attackers succeed in gaining also attentive users to unintended participation in the execution of malware. Therefore, IT administrators should not rely on classic AV solutions and firewalls alone, but rather implement IT security as an overall concept involving the users.

1.4.3 Ransomware

Ransomware is a word from the English terms ransom and malware. Ransomware is malware that restricts or prevents access to, or use of, data, applications, or devices, and only releases those resources against payment of a ransom.

Cyber attacks using ransomware violate the security goal of the availability of data and systems. At the same time, it is a form of digital blackmail.

There is a distinction between

- Ransomware that blocks or prevents the access and use of a device, e.g. by superimposing the display with an image or website and prohibiting normal operation, and
- Ransomware that encrypts user data using symmetric and / or asymmetric methods and promises the key used or a tool for decrypting the data against payment of a ransom.

The ransom payments are often processed via digital currencies such as Bitcoin and anonymous websites in the TOR-network.

The majority of the well-known ransomware families continue to target devices with the operating system Microsoft Windows. There are also some ransomware families, which attack the desktop operating system Apple MacOS or Web servers. Ransomware variants are also used for mobile operating systems such as Google Android.

In the field of desktop operating systems, mainly ransomware with encryption functions were detected since July 2016, while ransomware with a blocking screen like LeakerLocker was relevant for mobile operating systems like Google Android. In these areas, the situation did not differ from the previous year.

The primary attack vectors are still attachments of spam e-mails as well as drive-by attacks using exploit kits. In some cases, ransomware is camouflaged as a program update and the user is thus induced to installation. Ransomware for mobile platforms is mostly installed by the user (social engineering) or distributed disguised as a legitimate app via alternative app stores. However, these attack vectors are not new and are widely used to spread malware. A new attack vector in the area of ransomware is the exploitation of software vulnerabilities over the Internet and in local networks, which were used in May 2017 for the initial infection and further spread of the ransomware WannaCry.

Sabotage via Ransomware Petya

Situation
At the end of June, a malicious software called NotPetya / ExPetr spread worldwide in corporate networks. In individual cases, the attack had a massive impact on the production and critical business processes of affected companies. Several companies were also affected in Germany. The focus of the cyber attack was in Ukraine, where the first cases occurred, especially in critical infrastructures. In Ukraine, there have been several IT-controlled sabotage attacks on electricity networks, airports and the railway system. The first international cases concerned companies that had branch offices in Ukraine.

Cause and Damage
The malicious software used to encrypt data and to decrypt it against payment of a ransom. However, both technical and strategic features differentiated this malicious software from other ransomware families. ExPetr not only used the EternalBlue exploit, just like WannaCry. In addition, it also included a component that stole Windows passwords from an infected system's storage, as well as another legitimate administration tool that allows you to connect from one computer to another in a network. For example, ExPetr reached a number of business units relevant to production or operations.

Similar to WannaCry, security companies, government agencies and private security researchers have invested large efforts to analyse ExPetr. Within a short time, it was found that the initial distribution path was apparently a Ukrainian financial software called M.E. Doc. The website of the provider had been compromised, so that the malicious code was transferred to users of the software via the auto-update functionality.

When searching for ways to remove encryption without a ransom payment, several security researchers discovered that the ransomware functionality had not been implemented completely or roughly incorrectly in certain parts. This could be an indication that ExPetr was not intended as a criminal ransomware tool, but rather as a sabotage tool with strategic intent in the Ukraine. The distribution outside the Ukraine would then have been unintentional. This is consistent with the observation that ExPetr does not spread over the Internet but only searches for further victim systems in the internal network and in already open connections. As a sabotage tool, ExPetr is similar to Shamoon or KillDisk, making it impossible to start a computer by overwriting important hard drive parts.

Reaction
The BSI has carried out technical analyses, as well as an assessment of the known facts in the National Cyber Response Centre (Cyber-AZ). Corresponding information and warnings were given to the target audiences of the BSI. The BSI pointed out in its warnings that ExPetr is taking advantage of the lack of security in internal networks. It is spread with methods in networks, which are known as Lateral Movement and are used mainly by professional APT groups. Contrary to the concept of a "kill switch," the BSI recommends making sustainable configurations which basically prevent or at least hinder the lateral movement.

Recommendation
The cyber attack wave with ExPetr has once again clearly demonstrated how vulnerable critical business processes in companies and institutions are in a digitised world. The compromising of a single computer cannot always be prevented, but this should not lead to the failure of an entire network. The BSI therefore recommends segmenting networks, disabling local administrator accounts on computers, or at least providing computer-specific passwords. In addition, local administrators should not be able to log on to other computers over the network. In general, connections between workstations should be logged and data should be exchanged using specially configured file servers. However, sustainable measures also include the fact that providers of software must guarantee and maintain their update mechanisms and the security of their websites.

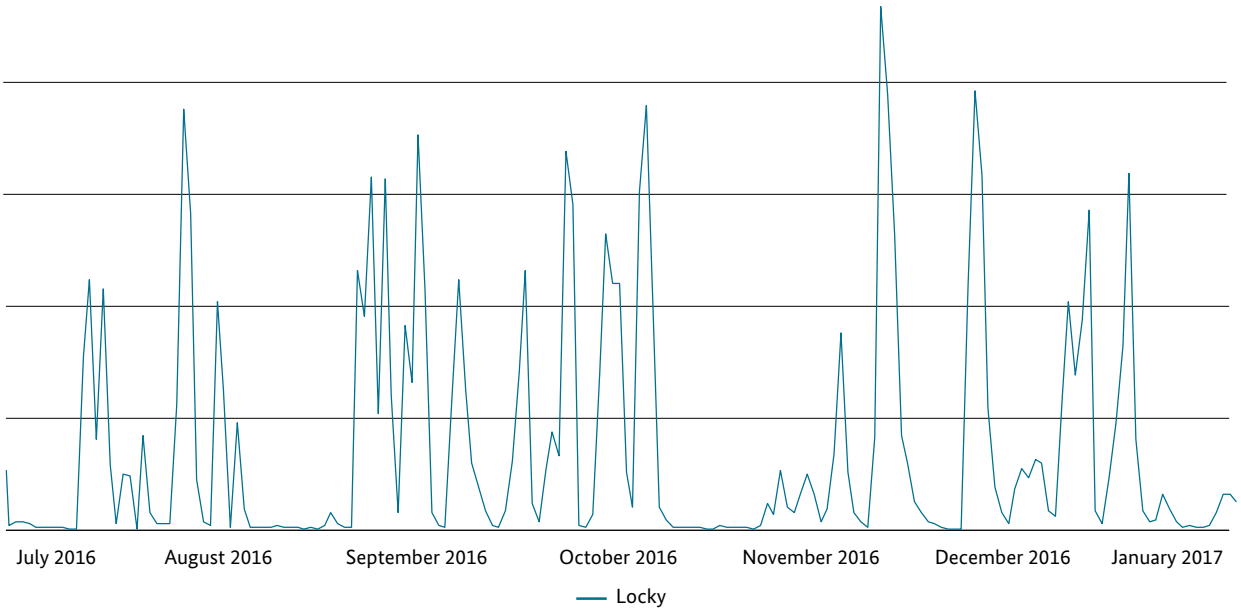


Figure 8 History of the number of attachments of spam e-mail messages analysed by the BSI from July 2016 to December 2016, which could be assigned to the ransomware Locky

Threat Situation Fluctuates Analogous to Spam Situation

The detection data for ransomware infections available to the BSI show that Germany in the reporting period was most frequently affected by the ransomware families Locky, Cerber, CryptXXX, Crysis, Petya / Goldeneye and the downloader Nemucod.

The actual threat posed by ransomware in Germany varies with the general spam situation. Almost daily, there are reports of new ransomware types and variants. The website https://id-ransomware.malwarehunterteam.com/ listed in early April 2017 over 350 families for ransomware with encryption function alone. However, this number does not play an important role in the actual risk situation for Germany.

Spam botnets such as Necurs are responsible for most spam e-mails sent to Germany. In the reporting period, there were repeatedly strong spam waves, which should infect users with ransomware. In addition, however, there were also periods of time when shipment of spam e-mail for implementation of ransomware failed out, once in November 2016, and once in the beginning of 2017 (see figure 8).

Most of the ransomware attacks were non-targeted mass attacks. In addition, there were also incidents suggesting a more targeted or manual approach during infection with ransomware. An example of this is the ransomware GoldenEye, which was used in December 2016 against various organisations in Germany, by sending alleged applications to actual job advertisements by e-mail (see info box ransomware in HR departments page 28).

As of 12 May 2017, infections with the ransomware WannaCry (see info box WannaCry page 26) occurred worldwide. In contrast to previous ransomware attacks, this malware spreads independently like a computer worm in the internal network as well as in the Internet without user interaction. The malware therefore uses a vulnerability in the SMBv1 protocol from Microsoft Windows, which was patched by Microsoft in March 2017 and became known in the framework of the shadow broker publications in April 2017. In a global comparison, the effects of WannaCry in Germany were limited. Infections were reported to the BSI in KRITIS companies as well as with several private users.

Another form of digital blackmail in the reporting period was attacks on insufficiently secured database systems. In doing so, contents was copied or deleted, and a blackmail message was left that the affected parties could retain a copy of the deleted data for payment of a ransom. At the beginning of 2017, among others, MongoDB, Elasticsearch, and MySQL installations were affected by these attacks.

WannaCry

Situation
The ransomware WannaCry in early May 2017 brought a great concern of the IT security community to life. A malicious program that encrypts files, making it impossible to operate systems and services until payment of an extortionary sum, combined with a vulnerability scanner that independently spreads the malicious software onto other vulnerable systems in the internal network without user interaction, became active. It was a "small version" of a crypto-worm.

Cause and Damage
An SMBv1 server vulnerability was exploited for which a patch was already provided by Microsoft in the middle of March and whose existence was later publicly known in the context of shadow broker publications. For various reasons, however, the patch was not implemented everywhere, with the result that unpatched systems were vulnerable to the attack.

In the case of WannaCry, the payment function, that is, the promised possibility of getting a decryption program against ransom, was faulty so that any ransom payment was in vain and there was little hope of restoration.

In Germany, Deutsche Bahn's attack was widely publicised, with display panels at railway stations failing and displaying the extortion message. Few other cases were publicly known. A few hundred systems are also infected with the double-pulsar backdoor, without the encryption becoming active. These were notified by the BSI via the providers. Internationally, the impact in individual countries was significantly higher. Above all, Russia was affected, but over 60 hospitals in the UK were also affected, directly affecting patient treatment.

Reaction
A surprising programmer error led to the fact that the domain, over which the encryption was triggered, could be "blocked" by a security researcher in the short term. Systems were therefore infected with a part of the malware, but the encryption was not going active. As a result, significantly greater damage could be prevented.

The challenge was that the actual path of infection was not able to be effectively tracked internationally.

The case of WannaCry was a clear example of how the cooperation works nationally in the National Cyber Response Centre, but above all with the international partners of the BSI: there was a close exchange regarding the respective concern, spread and (non) effect. The CSIRT network of all European CERTs, which has just been established within the framework of European legislation (EU-NIS Directive), is also cooperating for the first time across countries in a specific case.

However, the situation shows that such worm-like events with a sabotage function are not fiction, but actually occur and lead to considerable damage despite the many warnings and recommendations to safely implement systems. Only rapid reaction has kept the actual damage far more contained than its possible extent.

Recommendation
Basic recommendations against ransomware software are:

- Keep your system on the current patch level so that no weak points can be exploited. For this purpose, manufacturers offer services for private users. For commercial users, clauses should be included in the IT service contracts for the fastest possible testing and patching.

- Periodically secure your own data and critical systems to reduce the temptation to need to respond to the demands of extortionists. You can then restore your systems as soon as possible with the least possible losses. Also check the backups regularly for re-usability and practice the process.

- Separate your network into sensibly small segments, so that the threat on a system cannot lead to a complete infection of the entire company / authority network.

For more information and recommendations for action against ransomware, the BSI has summarized a dossier, which can be downloaded from the BSI website.

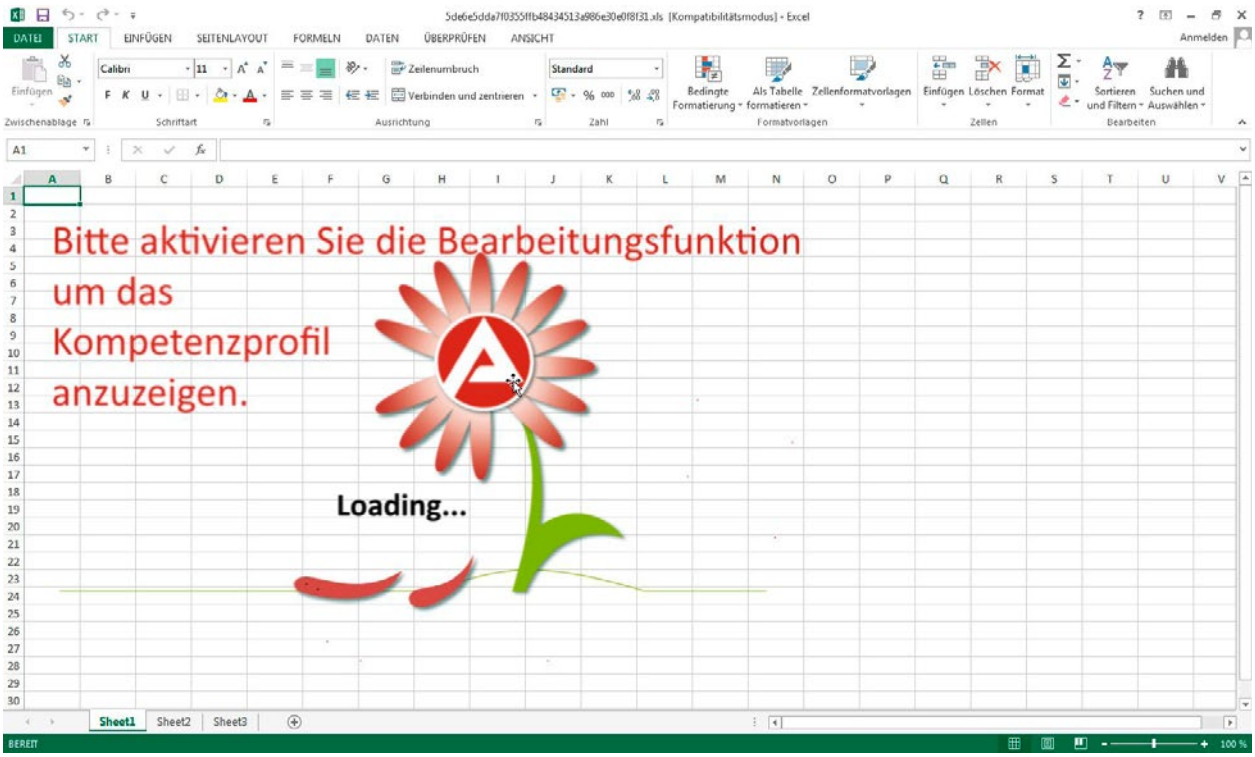


Figure 9 Screenshot from the ransomware campaign Goldeneye
(File name generated by analysis environment, original: “Application” + First name + Last name + “xls”)

Continuing Business Model for Cyber Criminals

Ransomware is a well-established and successful business model for cyber criminals. Today, ransomware is preferably used with encrypting functions. The large number of observed ransomware variants shows that there are still investments into ransomware. Therefore, it can be assumed that this type of malware will remain a relevant threat in the coming years.

Further information on ransomware was compiled by the BSI in July 2016 in a comprehensive situation dossier on the issue of ransomware. The dossier is available on the BSI website and defines the types and functions of ransomware, presents the attack vectors and describes protection measures from the fields of prevention, detection and response.

Ransomware in HR Departments

Situation
In December 2016, cyber criminals sent out targeted fake e-mails with alleged applications to employees in company HR departments. The e-mails contained a PDF and an Excel document as attachments. In the PDF document that looked like a real application, HR managers were personally approached and reference was made to an actually open position in the respective company. The Excel document with the alleged application folder contained a malicious macro. When the document was opened, the recipients were prompted to activate the "editing function" and thus the execution of macros.

Cause and Damage
If a recipient responded to the call on a PC with Windows operating system, his PC was infected with the ransomware "Goldeneye". This is a further development of the ransomware combination "Petya / Mischa," which in March 2016 also spread with fake applications. Goldeneye encrypts files and modifies the boot sector of the hard drive. Access to the system or the data is then no longer possible. Victims were asked to pay a ransom of around EUR 1,000 in the form of bitcoins to the perpetrators via the Internet in order to receive a decryption program. While in Petya / Mischa a weak point in the implementation of the encryption allowed the data to be decrypted even without payment of the ransom, this was no longer possible with the further development Goldeneye.

Ransomware is a business model for cyber criminals now well established for many years and affects desktop operating systems like Microsoft Windows and Apple Mac OS, server systems under Linux as well as mobile operating systems like Google Android. Infection vectors of ransomware for desktop systems are currently mainly e-mail attachments or drive-by attacks using exploit kits. In the case of ransomware incidents, failures in the prevention process are clearly identified: poorly maintained systems, missing, outdated or untested backups, weak administrator passwords and lack of network segmentation considerably facilitate the attack and lead to significant damages.

The extent of the damage depends on how the affected institution is technically and organisationally prepared: even if preventive measures will fail and cannot avoid the disruption, a good coping strategy can considerably limit the damage.

Reaction
The sooner an organisation's IT security officers are informed of possible signs of a cyber attack, the more likely they are to initiate the search for the polluter devices. And the sooner the polluters are found, the faster they can be shut down and the encryption process aborted. If the IT team can ensure that all infected devices have been identified, shutting down or isolating these devices can also ensure that the threat is neutralised.

Recommendation
The BSI has published on its website the "Situation Dossier ransomware," which contains numerous concrete aids for prevention and reaction in the event of damage. In order to prevent data loss, users should create backups in advance from which data can be restored. To prevent infection by ransomware from the start, existing vulnerabilities in used software should be closed and users should be made aware of the topic. The corporate network should be segmented so that a single infection cannot spread to the entire network.

1.4.4 Botnets

Botnet infrastructures provide cybercriminals access to large resources of computing capacity and bandwidth that they can use for their criminal activities. Due to the professionalisation and commercialisation of cyber crime, the operation of a botnet can also be implemented comparatively simply and inexpensively by technical laymen.

Also in 2016 and 2017, botnets were used on a large scale for information theft, for distributed denial-of-service attacks (DDoS attacks) on computer systems, for spam sending and distribution of malware. The underlying bot software is generally modular and can be used flexibly for various attack purposes without the need for a new infection of the attacked system.

During the reporting period, up to 27,000 bot infections of German systems were registered daily by security researchers and reported to the German Internet providers via the BSI. The providers inform their customers about the infection and offer in part also help with the clean-up of the systems.

Focus Online Banking Fraud

The reported infections spread to 108 different botnet families in the reporting period. A closer look at the twenty most common families in early March 2017 shows that the majority is primarily used for online banking fraud. Dropper, who only serve to reload other malware, follow second. In the further ranks are found botnet families for click fraud or bitcoin mining, Spam sending and DDoS (see also info box Mirai page 31).

Due to its high market share, mainly Microsoft Windows systems are affected by bot infections. The following figure shows a distribution based on a sample at the end of March 2017. The botnet families which transmit the operating system of the victim system to a sinkhole server are used as data bases. The high percentage of current Windows versions shows that even new protection mechanisms of the operating systems do not provide a sustainable protection against infections.

In addition to Microsoft Windows, other operating systems and hardware platforms are increasingly becoming the focus of cyber criminals. Currently, about ten botnet families are known, which focus exclusively on Android and are used for information theft. One in six botnet networks observed for Windows devices also has a malware component for Android systems. They are mainly used for online banking fraud in order to catch the

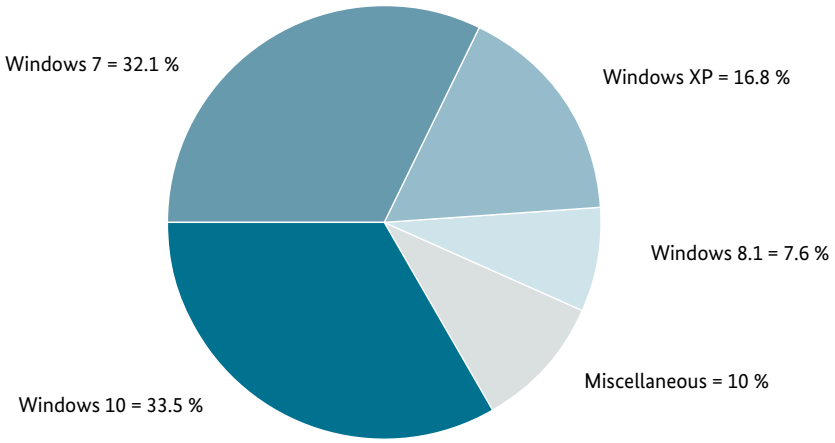


Figure 10 Operating systems of infected systems, random sample 29/03/2017

TAN sent by SMS in the mTAN procedure. At the end of March 2017, six percent of reported victim systems were an Android system. The majority of the Android infections can be attributed to malicious apps, which were obtained from third-party sources.

In addition to Linux-based web servers, devices of the Internet of things such as home routers, surveillance cameras or internet-capable multi-media devices are increasingly compromised and integrated into botnets. Simultaneously, compromised systems based on Mac OS X were observed.

Successful Defence

In order to detect botnet infections, security researchers use so-called sinkhole systems, which receive the contact requests from bots instead of the regular command & control servers (C & C servers). This is possible by registering the domain names used or the IP addresses. Since not all globally available botnets can register valid C & C addresses for sinkhole systems, the 27,000 infections reported in the reporting period represent only a minimum for Germany. The level of visible infections is mainly determined by the type and number of Sinkhole

Smashing the Botnet Infrastructure Avalanche

Situation
On 30 November 2016, the central criminal inspection of Lüneburg and the public prosecutor Verden successfully dismantled the Avalanche botnet infrastructure in a spectacular international operation. The BSI decisively supported them. The botnet infrastructure servers were shut down, perpetrators were arrested and users of infected systems were informed by Internet service providers.

Cause and Damage
Avalanche was the largest botnet infrastructure ever known. More than 20 botnet families were identified. An international group of perpetrators had infected a hundred thousand private and commercial computer systems with different malicious software. The perpetrators used this infrastructure to spread spam and phishing e-mails as well as malicious software such as ransomware or banking trojans.

Reaction
The successful action is the result of a four-year intensive investigation and analysis work. Authorities and institutions from more than 30 countries participated in the campaign, including the BSI, Europol, the FBI, the non-profit organisation Shadowserver and the Fraunhofer Institute for Communication, Information Technology and Ergonomics (FKIE). The international cooperation in this action resulted in six arrests, 37 house searches and the confiscation of 39 servers in several countries. 221 more servers were shut down by the hosting provider. Over 830,000 botnet domains were confiscated or redirected to so-called sinkhole servers. Systems with active infections now connect to these sinkhole servers and no longer receive any control commands. Information on the infections recorded at the sinkhole at German IP addresses are made available to the responsible Internet providers. They can then inform their customers in writing about the infection. In this way, only customers whose systems are currently infected and whose IP addresses could be identified during this action are informed. In total, the BSI assumes several thousand affected German users. Information on affected foreign IP addresses is forwarded via the CERT-Bund to the relevant national CERTs in more than 80 countries around the world in order to be able to inform affected users also there.

Recommendation
Even if the botnet infrastructure has been switched off, the infected systems at the end users can only be cleaned by themselves. Users who have been notified by their Internet service provider should check their devices for an infection with malware and close vulnerabilities. The malware on the affected systems were not deleted by the destruction of the botnet infrastructure. It can therefore not be ruled out that the perpetrators will again reach control of the respective botnets at a later date. Affected persons should therefore act as soon as possible. The deactivated botnets existed, according to current knowledge of the BSI mainly from Windows systems and Android smartphones. However, an infection cannot be excluded with smartphones with Apple iOS, Microsoft Windows Phone or operating systems such as Apple Mac OS X or Linux.

addresses registered by security researchers and fluctuates therefore very strongly. Based on the experience gained from successful botnet disconnections, it can be assumed that the dark figure is significantly higher and moves at least in a six-digit range.

The successful strike against the Avalanche botnet infrastructure (see info box page 30) has forcefully demonstrated that a successful fight against botnets requires the collaboration of law enforcement, authorities and security researchers, and that three pillars must be addressed at the same time:

I. Switch off the infrastructure and sinkhole the malware domain

II. Investigations against criminals with arrests and raids

III. Information of affected persons with infected systems

As part of the takedown of the Avalanche infrastructure, end users are required to clean up their systems. Since end of November 2016, attempted bot accesses on former Avalanche servers are redirected to a sinkhole server. The access attempts are reported by the BSI to the German Internet providers, so they can inform their customers. The cleaning of the customer's computers can only be done by the respective users, neither the provider nor the BSI can take over this task. The sinkholing of the malware domains is expected to end by the end of 2017. If users have not cleaned up their systems by then despite notification, there is a risk that criminals will take over the inactive but still infected systems. It is already clear that the clean-up of all end systems is a big challenge and many users do not react despite notification. Thus, seven months after the beginning of the sinkholing and the consistent information of the affected parties by the Provider, more than 2,100 IP addresses are still reported to providers in Germany every day. This corresponds to about 46 percent of the infections originally detected in Germany. In the meantime, the highest observed infection value was even 13,340 unique IP addresses. According to the detected IP addresses, over 62 percent of the systems are still infected unchanged.

Since June 2017, the Law on Implementation of the European Directive to Ensure High Network and Information Security (NIS-RL) has given telecommunications providers additional powers to remove such infected systems from the network.

Threat Situation Continues to be High

As the latest developments show, the threat situation by botnets remains high compared to the previous year. In 2016, the IoT botnet Mirai impressively illustrated the threat posed by the internet of things in this context (see info box Mirai page 31). On the one hand, the high number of inadequately protected, publicly available systems is noticeable, on the other hand it shows the impact strength of the attacks originating from this kind of botnets.

Due to the publication of the Mirai source code in the autumn of 2016, numerous further Mirai developments have emerged, which are continually trying to find and acquire new victim systems. This source code can now also be used by adolescents without any computer skills known as script kiddies. As a result, botnets from IoT devices have become normality. Together with the fact that with Necurs one of the largest known botnets has DDoS functionality, the probability of occurrence and the impact of DDoS attacks have increased.

Mirai

At the end of September 2016, the Mirai source code was surprisingly published. It was the complete source code, including a guide, so that even amateurs could easily expand and convert it into executable code. Part of the source code were also lists of identifiers and passwords of vulnerable IoT systems. A user under the pseudonym "Anna-senpai" explained that the malware had done their service for him and he would withdraw from the DDoS business. Since then, the source code has been widely distributed unhindered and used for various further developments, so that currently several hundred botnets of different size and design exist, which have been expanded and technically optimised in the range of functions.

1.4.5 Advanced Persistent Threats (APT)

The term "Advanced Persistent Threat" (APT) is often equated with intelligence services. The aim of APTs is typically to obtain information in the government or general economic interest. The approach is targeted, takes place over longer periods of time, and often requires greater personnel strength because of large manual efforts. All this is consistent with the characteristics attributed to intelligence services.

However, there are also indications that some APT campaigns are not conducted directly by intelligence services, but rather by well-organised non-governmental groups.

APT Attacks by Commercial Service Providers

Security companies have repeatedly reported large-scale, worldwide cyber espionage campaigns over the past few years. However, several of these campaigns were very unspecific in the selection of industries and governmental organisations. It was therefore doubtful that a concrete intelligence service could have an interest in this broad target selection. In addition, there was the observation that some groups were also active on weekends and during (local) night times. Both of these phenomena are seen by security companies as an indication that such campaigns are carried out by service providers. In the English-speaking space, terms such as "Contractor," "Hackers for hire" and the striking "Gunslingers" have prevailed.

One of the first assumptions that the attacker could be an independent service provider dates back to the report from the US company Symantec about the group Hidden Lynx (September 2013). Also, the groups APT3 / GothicPanda and Nitro / DynamitePanda are classified as service providers by security companies. It is conceivable that several intelligence services of the same state access the same service provider.

A similar form are so-called APT boutiques, which develop professional cyber espionage software and sell it to companies or states. There are different forms of transparency. While companies such as FinFisher or Hacking Team do not conceal the fact that they are developing and selling such software, there are also developers like the Poseidon group discovered by Kaspersky, which act rather covertly and sell their services not to governments, but to companies ,

While the concept of "contractors" suggests a legal constellation (in the sense of the client), there are also APT groups, which have a strong overlap with criminal activities. An example of this is the Winnti group, which was named after the malware through which it became known. The perpetrators have been generating so-called "fake anti-virus malware" since 2007, in order to persuade victims to pay a license for fake security software. Around 2013, Kaspersky showed in an analysis of how the Winnti Group attacked game vendors, but this also with clearly financial interests. Since then the attacks have been diversified by means of Winnti and have also been observed in incidents with companies which are more of a cyber-espionage character. In 2016, for example, it became publicly known that it has come to data outflows at a German industrial company through Winnti.

Blending of Interests

These examples show how fluent the boundaries between crime and cyber espionage are. It is even possible that intelligence services from a state use the comparatively comfortable and professional malware Winnti to give their activities the appearance of purely criminal activities. For example, the security company FireEye reported that, following US legal and diplomatic action against China, the observable activity of most of the APT groups attributed to China has greatly declined.

The blending of financially motivated criminal groups and states would be most significant if the assumption expressed by security companies confirmed that the Lazarus group had carried out counterfeit transmissions in the SWIFT network of the banks on behalf of the North Korean state. A similarly clear mixture is shown by the fact that the criminal GameOver-Zeus botnet used in the online banking fraud in the Ukraine was fed with search terms that point to espionage. Security researchers suspect that the operators of the botnet have worked with these search terms on behalf of an intelligence service.

The fluid boundaries between APTs and crime ware also mean that espionage attacks are now also used in criminal campaigns. For example, the Carbanak Group operates the so-called Lateral Movement in its attacks on banks in order to spread within the internal network until it can trigger fictitious transfers. Even with ransomware such as Samsam, Lateral Movement was observed: the perpetrators spread through the internal network until they found servers that contained sensitive data so that encryption of the data would very likely result in payment of the ransom.

Difficult Attribution

These facts show that there is a structural overlap between criminals and intelligence services in cyber espionage. Both criminals and state actors are capable of professional attacks. The commissioning of criminal groups through intelligence services is also conceivable. Since techniques and apparently also malicious code are exchanged, some can no longer distinguish easily between crime attacks and espionage attacks using the methods used in the case of profound network compromises. There is a need for time-consuming technical analysis of a lot of information on specific incidents in organisations, as well as a series of findings and measures outside the cyber space in order to make a reliable assignment to perpetrators.

However, the technical countermeasures are largely identical in both areas. For example, the measures described in the ransomware dossier of the BSI to protect against malicious mail attachments also increase the protection against many targeted attacks. As a first step, perpetrator-agnostic security measures should be implemented. This includes both preventive measures and measures for the detection of successful compromises. Only after these measures have been taken will it be possible to analyze one's own exposure and risk situation and purchase threat intelligence to complement the current monitoring solutions with signatures and information.

1.4.6 Social Engineering

Whenever attackers do not manage to compromise vulnerabilities by means of technical attacks due to current software, firewalls and virus scanners, they focus on the human factor as the weakest link in the security chain. Analogous to the classic trick fraud, attempts are made to manipulate the victims to install malware or to issue sensitive data. The different variants of this Social Engineering approach use strategies such as the pretending of a personal relationship with the victim, promise to win a prize or offer other lucrative opportunities, for example, at online shopping.

Targeted Attacks on Companies or Employees

In the last few years, mostly widespread phishing campaigns have been carried out which, for example, lure with a prize draw or provide simulated information about a package delivery. Today, the proportion of targeted phishing attacks – the so-called spear phishing – is significantly greater, with which are addressed individual companies or employees. Attackers use a variety of public sources, such as the company website or social media, to collect as much information as possible about the targeted company and the respective employee to make phishing mails then look as authentic as possible. These targeted phishing attacks are no longer exclusively done via e-mail, but are increasingly flanked by establishment of contact in social media or telephone calls, which simulate a known identity to the victim. To make the appearance of trustworthiness, the attackers frequently rely on the reputation of established companies or brands. For this purpose, goods are sold in sales platforms or manipulated apps are published in app stores. In many cases also the name of well-known authorities or other public institutions is abused with social engineering. This lowers the victim's inhibition threshold to click on a link or attachment, or to deviate from the usual payment method in a marketplace.

Phishing attacks are increasingly being observed in areas where it is common to receive e-mails from strangers. This is particularly the case with the widespread malicious e-mail campaigns with a focus on personnel departments, which refer to real application procedures.

A common attack method is also the support trick, in which callers masquerade themselves as call centre employees of renowned manufacturers such as Microsoft, Dell or Lenovo. On the pretext of trying to solve a problem recognised by the manufacturer on the victim's computer, the victim is tempted to install a remote maintenance software. If the victim follows the instruction of the alleged technician, the attacker gains complete control over the victim's computer.

Awareness as a Useful Antidote

Social engineering is still a frequently used method for attackers. This is explained in particular by the fact that the attack vector via the "human weak spot" does not need to exploit vulnerabilities in hardware or software or to circumvent technical safety measures. The BSI has therefore warned against these attack methods for many years.

Spear Phishing against Executives

Situation
In June 2017, the BSI monitored professional cyber attacks on private e-mail mailboxes from executives in business and administration. With this campaign, deceptively genuine spear phishing mails were sent to select executives. The attackers claim to have noticed anomalies with the use of the mailbox or to offer new security functionalities. The user is prompted to click on a link and to enter his password on the web page that opens. The campaign was targeted against Yahoo and Gmail accounts. As early as 2016, the BSI was able to observe that websites were registered which are suitable for spear phishing attacks against customers of the German webmail service providers gmx.de and web.de and whose infrastructure resembles the current campaign. Although these domains were not the target of the attacks in June 2017, it shows that the perpetrators also identified these e-mail providers as a possible attack path.

Cause and Damage
With password disclosure, the perpetrators get access to a victim's personal e-mail mailbox and its contents. In this way, the attackers have the possibility to gather further information, possibly also officially, about the target person and to use these for later targeted attacks. By accessing the mailbox, the attackers can also communicate in the name of the user and misuse his identity.

Reaction
In the government networks, the BSI was able to ward off an attack by the campaign. In principle, phishing e-mails of this kind can be detected and repelled very effectively in government networks. However, the protection of private e-mail mailboxes of function providers is beyond the competence of the BSI or the respective organisation. Executives in administration and business should therefore ensure that their private mail accounts are also secured. This is an important part of digital personality protection.

Recommendation
Digital personality protection is the protection of the activities of important personalities in the digital space. In addition to the protection of private e-mail mailboxes, this also includes measures such as the verification of Twitter and Facebook accounts. The following measures protect not only against targeted spear phishing attacks on executives, but also against large-scale, less professional criminal phishing attacks:

- Business content should not be communicated and processed through private mailboxes.
- E-mail communication should be encrypted.
- Users should use two-factor authentication. Some webmail service providers already offer this functionality.
- In principle, passwords should not be entered on web pages that were linked from e-mails.
- E-mails that indicate a targeted attack against the business function should not be deleted, but shown to the IT staff of the organisation.
- If the password was entered on a non-trusted page, it should be changed on the original page if in doubt.

The BSI supports executives from government and politics directly to implement these measures.

An increasing professionalisation of the attacks is currently being observed. It makes it increasingly difficult for employees or technical systems to identify them. Companies increasingly rely on awareness-raising measures to train employees. Usually, however, these trainings are offered only sporadically, that means, there is a lack of regularity and timely reference to current methods and variants of the attackers. Comprehensive protection against social engineering can only be achieved through continuous sensitisation measures integrated into an overall concept.

1.4.7 CEO Fraud

CEO fraud is a variant of social engineering which is operated by the attackers with great effort. This increased expenditure is explained in particular by the potentially significant damage sums which criminals can achieve and which in individual cases can amount to millions of euros. The BSI has found that this fraud scheme is used more and more professionally.

In the case of the CEO fraud, target acquisition is enacted in a high degree. One of the technical basic skills of such attackers is the acquisition of information about companies and employees. To this end, different sources are used: the company website, press and stock exchange announcements, entries in social media and in the commercial register. There are also cases in which the attackers contacted employees by telephone in advance to get contact details and further details about the company. In some cases, techniques are also used to simulate the victim a known telephone number when a call is made.

In addition, the e-mails sent to the victims are prepared and delivered with great professionalism and care. The attacker masquerades himself as CEO, CFO or comparable member of the management, and tries to tempt the victim to the fastest possible and simultaneously confidential transfer of large amounts of money. In order to convince the victim of the authenticity of the request, the attacker often uses correct sender addresses and imitates the real e-mails from the executive floor regarding wording, signature and pictures very well to that extend that nothing unusual is noticed at first sight. Frequently, real existing employees are also given as a reference for verifying the legality of the transaction, which the victim, however, does not contact due the simulated time pressure.

In part, the urgent payment instructions in the e-mails are supported by telephone calls from the alleged employee of the management level or an added “consultant.” In order for this fraud attempt to succeed, attackers and “consultants” put high time pressure on the victim by making the business success or even the existence of the company dependent on the timely transaction.

1.4.8 Identity Misuse through Remote Identification Procedures

In order to be able to identify their customers in online transactions, banks, telecommunication companies or other service providers are increasingly offering online procedures. While a high security level can be achieved with the online identification function of the ID card, procedures are increasingly being introduced to the market, the security of which cannot reach the level of a personal identification and verification of an ID document.

Unsafe Identification via Video Channel

In particular, the increasingly offered procedures intended to enable identification within a video chat offer potential abuse. A video image of the user and his identity card recorded with the smartphone is not comparable with identification in the case of physical presence with regard to uniqueness and security. In any case, a video channel can be used to test at least security features which change with certain light conditions while the ID card is moving, such as the holographic portrait or the laser tilting image on the back of the German ID card. Haptic features or even the infrared or ultraviolet light appearing safety features cannot be checked remotely.

In security analyses the BSI has demonstrated that it is already possible with standard equipment to create a false identity card and to generate the impression of corresponding individual, optically variable security features as part of a video transmission in real time.

CEO Fraud

Situation
Numerous cases of CEO fraud have been reported to the BSI. Those affected include critical infrastructures and authorities. For example, an employee of a German state authority was personally "commissioned" to carry out a "confidential financial transaction" of EUR 961,000. The mail traffic, allegedly coming from the President of the authority, was accompanied by an appeal from an alleged lawyer, which was intended to lend emphasis to the request. The highest damage in a single case known to the BSI amounted to a loss of EUR 40 million for an automotive supplier. In the first half of 2016 alone, a European bank reported 50 cases of CEO fraud from its customers. Altogether, the attackers tried to steal more than EUR 20 million. In 20 of these cases, the attack was already prevented in the company. In 20 other cases, payments were stopped by the bank or could be recovered. In the remaining ten known cases, a total loss of EUR 5 million was incurred. The positive figure is much higher.

Cause and Damage
In the case of CEO fraud, victims are contacted both by e-mail and by telephone. The aim of the attacker is to induce a company's employees to transact a large amount of money from a business account to a third-party account. Target audiences include, in particular, financial and accounting employees who have access to company accounts. The focus is increasingly not only on international companies, but also on medium-sized companies.

Reaction
In case of doubt, the personal contact with the alleged sender of the e-mail should always be sought. In addition, in such cases the fraud attempt can be detected if the reply button of the e-mail program is not used to reply to the e-mail, but rather a new e-mail is sent to the address of the person named in the e-mail. This can be used to counter masked sender addresses. Furthermore, bulk receiving of such e-mails can be detected by monitoring, so that the sender's address can be blocked.

Recommendation
Protection against CEO fraud provides training that makes employees aware of fraudulent and manipulative behaviours. The focus should be on employees from critical areas, such as accounting. As a precautionary measure, the four-eye principle is recommended for payment instructions in order to establish additional security.

Implementing Recommendations

In order to make erroneous identification more difficult, providers of video identification procedures should implement at least the following recommendations that the BSI has developed together with providers and other stakeholders:

- Secure communication (mandatory end-to-end encryption of the video connection, implementation of the recommendations of the BSI Technical Guideline TR-02102)
- Matching of form and content of the optical security features with the characteristics contained in the identity card and references (by means of still images or by technical support)
- Random prompt to cover and move the ID card and the face or head, check for artefacts by means of a cut-out magnification
- Psychological questions and observations in the process (plausibility, intention of the person acting)
- Automated validity and plausibility checks of ID data

In order to be able to uniformly assess the security level of different procedures for identification, the BSI has drawn up a technical guideline. This makes it possible to select from different equally suitable procedures of a certain confidence level (according to eIDAS regulation). The guideline can be used as the basis for a uniform assessment, e.g. by accredited conformity assessment

bodies. This creates legal certainty for service providers and avoids application-specific additional requirements. In appropriate technical legislation, it is then only necessary to determine the level of confidence required for the specific application.

Due to the vulnerabilities described, it is to be assumed that video-based procedures, even with the additional measures mentioned, cannot reach the high level of confidence that is possible in the personal identification or use of the online identification function of the ID card. Therefore, video based processes should not be used to identify persons in security-related areas.

1.4.9 Cryptography

Cryptography continues to be a key component of the effectiveness of many IT security mechanisms. Current cryptographic mechanisms provide excellent security guarantees. Two parties that reliably control their local computers and do not share a secret can establish a secure connection across a network, even if the entire network is controlled by an adversary. When using strong methods, the computing power available to the adversary is largely irrelevant.

However, different aspects can lead to a cryptographic system failing in practice. These include:

- lack of endpoint security
- faults in implementations
- errors on the level of protocols
- security problems related to backward compatibility of protocols used
- problems with the initial distribution of public keys or a lack of consistency between security objectives and security guarantees of the cryptographic mechanisms

In particular, errors in widespread implementations can compromise the security of many systems. The fact that many systems do not or seldom receive software updates or are not taken into account in security analyses also ensures that vulnerabilities can also occur in productive use long after their discovery. This last point concerns, in particular, embedded devices (Internet of Things), hardware components of larger systems with their own firmware or mobile Internet devices. In addition, there are a number of attack paths that are primarily intended for targeted attacks on individual users, for example, the extraction of key material by side-channel analysis of an implementation or by fault attacks.

It is also problematic if the attacker has crypto-analytic capabilities that go qualitatively far beyond the state of public research. In the area of public key cryptography, also practically all security guarantees are lost as soon as the adversary has a scalable universal quantum computer since the underlying mathematical problems (factorisation and discrete logarithm) could be solved by Shor's algorithm on a quantum computer in polynomial time.

Security Requirements

Even when using cryptographic systems, various prerequisites must be fulfilled in order to achieve the desired security objectives:

- The parties involved must control their own computer systems, the cryptographic endpoints must be protected against foreign control or other compromise.
- At least once, a trustworthy distribution of some public keys must be ensured by other mechanisms
- At the endpoints, communication must not be able to be monitored directly, for example, via compromising emission or by the use of intercepting devices.
- The implementations of cryptographic procedures must be mathematically correct and, moreover, hardened against attacks on the implementation level.
- The cryptographic protocols used must not contain any vulnerabilities. This is much more difficult to accomplish for complex protocols than the security of the basic cryptographic features used, such as block ciphers or public key encryption.
- The security guarantees for modern cryptographic mechanisms are usually very strong, but technically also very specific. If security objectives and security guarantees of a cryptographic protocol are not exactly the same, vulnerabilities can occur.

Collision Attack on SHA-1

Situation
SHA 1 (abbreviation for secure hash algorithm) is a standardized cryptographic hash function, which has been widely used for many years. A hash function is used to calculate a unique hash value for digital data such as messages. The idea behind it: If two messages have the same hash value, they are identical. Hash functions are therefore used, for example, as the basis for creating a digital signature.

On February 2017, Researchers at Google and the University of Amsterdam have published relevant information on a practical collision of the hash function SHA-1.

As an example, researchers created two PDF files with different content, but the same SHA-1 hash value. The BSI had already generated such PDF files for the now outdated hash function MD5 in 2005.

Cause and Damage
The effort for this collision is still enormous, but it is about 100,000 times faster than a brute force attack ($2^{63.1}$ instead of 2^{80}). The authors estimate the cost of computation of a collision to be between USD 75,000 and USD 120,000, based on the cost of the required GPU computing time for the Amazon EC2 service.

Recommendation
This practically demonstrable attack on SHA-1 again shows how important it is to no longer use this hash function in applications that require collision resistance, e.g. signature generation. For many years now, the BSI has recommended that SHA-1 no longer be used for the above-mentioned applications, but to use current hash functions, for example, the SHA-2 family.

High Security Standards

Apart from a few exceptions, cryptographic algorithms reflecting the current level of cryptographic knowledge can be regarded as secure. For guidance, the BSI publishes the technical guideline TR-02102. Even a lot of somewhat older procedures offer a high degree of safety when used correctly.

A classical, mathematical cryptoanalysis is hardly successful with modern encryption methods. It remains important in practice, however, because uncovering theoretical vulnerabilities in cryptosystems is a kind of early warning system that helps to avoid practical problems. In addition, cryptoanalytic advances have the potential to comprehensively void the security guarantees of a procedure. However, it is generally unlikely that cryptographic methods, which are currently estimated by public research as state of the art, can be cryptoanalytically broken in practice, for example, by foreign intelligence services.

In addition to the legitimate use of cryptographic methods, criminal use has also recently become the focus of the public interest, for example in connection with ransomware. The use of cryptographic procedures for criminal purposes, such as the arrangement of unlawful acts, can hardly be technically prevented. The prevention of criminal applications (especially crypto-trojans) is achievable to a certain extent if state, business and society are enabled to configure their systems and their communication among themselves as securely as technically possible. Last but not least, the Digital Agenda of the Federal Government provides the goal of making Germany the number one counting for encryption site.

State of Development of Quantum Computers

Current information security is based, among other things, on public-key methods such as RSA, ECDSA or Diffie-Hellman, which could be broken using a quantum computer. This danger has been publicly discussed due to warnings by the NSA and a current NIST standardisation process for quantum computer-resistant cryptographic procedures.

A universal quantum computer that would be able to use Shor's algorithm for currently used key lengths and public key methods does not exist. In recent years, however, significant progress has been made, at least in the area of relevant basic research. In order not to be overtaken by this development, the preparations for the post-quantum period must start today. Particularly affected are confidentiality services with a long-term protection requirement as well as signature certificates with long periods of validity.

In addition to the possible additional protection of classical public-key cryptography by selected symmetric cryptographic methods, the main focus is on the development of quantum-computer-resistant public-key methods whose mathematical basic problems cannot be solved efficiently by a quantum computer.

In the future, a higher level of research and standardisation activities can be expected in the area of quantum computer-resistant cryptography, such as the "Post-Quantum Cryptography Project" initiated by the National Institute of Standards and Technology (NIST), begun in 2016. An important task for the BSI in the coming years will be to actively support these activities and to implement its own projects. In a study commissioned by the BSI, researchers from the University of Saarland and the Florida Atlantic University will provide a sound assessment and reliable forecast according to the current state of development and the potential future availability of a quantum computer. In concrete terms, current technological approaches and quantum-algorithmic innovations are intensively examined and their implications discussed in the context of current public-key procedures. The findings of this study are intended to enable the BSI to identify the need for action regarding the development, standardisation and dissemination of quantum computer-resistant cryptographic procedures.

In addition to quantum computer-resistant cryptographic methods, methods from the field of quantum cryptography are also mentioned as a possible solution for establishing secure data connections in a world with quantum computers. These are technical systems that solve a similar security problem by means of physical effects as public-key cryptographic methods do in a mathematical way. In particular, quantum cryptographic methods require special hardware for the data connection and a classic cryptographically authenticated channel for key negotiation. In addition, the security guarantees of such procedures are strongly dependent on implementation aspects. Therefore, quantum cryptography is currently not regarded as a practical or more secure alternative to post-quantum methods. However, there are internationally visible development and research projects, in particular, a quantum cryptography program with space-based components (satellites) in China.

1.4.10 Side-channel Attacks and Random Number Generators

Good random numbers are a prerequisite for the security of cryptographic mechanisms. They are required in particular to generate the keys for the cryptographic methods used in the transmission and storage of critical data, for example nonces (random numbers used once), AES keys or RSA moduli. Even cryptographically strong mechanisms can suffer a significant loss of security or even be broken due to a weak random number generator.

Side-channels have played an important role in science and the semiconductor industry for two decades and are also being considered as part of common criteria certifications and approvals. Cryptographic algorithms and protocols are in the design process commonly examined only as mathematical, abstract entities. However, as soon as they are installed in real crypto-devices, new attack vectors come along. Such attacks, for example, attempt to take advantage of the observation of the device while it is performing operations with or on secret data. The information derived from physically observable variables such as electromagnetic radiation, power consumption, runtime behaviour of individual operations and cache access times within the framework of such a side-channel analysis either already provide the key searched for or can be used as a parameter (apart from secret texts and possibly also cleartexts) for cryptoanalysis.

The BSI has defined functionality classes of random number generators for various purposes for the support of manufacturers, testing and validation laboratories and evaluators. The use of these classes is, among other things, mandatory within the framework of a Common Criteria certification in the German scheme. For example, physical random number generators of chip cards certified in Germany according to Common Criteria must be conformant to one of the defined classes.

In addition, the BSI took part in a long-term study of the random number generator (/dev / random) of various Linux kernel versions that were examined. The study results are available on the website of the BSI. The BSI also looked into the question of whether random numbers of sufficient quality can be provided considering the increasing use of virtual machines, especially in cloud-based solutions.

1.4.11 Other Attack Methods and Means

Technical Interception Systems

Calls that are conducted via mobile devices can be intercepted or recorded in various ways. In addition to the official lawful intercept interfaces of the network operator used, for example, by law enforcement authorities, unauthorised third parties with so-called false base stations or by exploiting vulnerabilities in the SS7 signalling can also record the contents of the conversations. SS7 stands for “signaling system number 7” and is a historically grown family of protocols. They are used, for example, in the connection setup in the case of roaming, if signalling is necessary between different components of the mobile radio networks.

Encryption can be Disabled

Calls and data are usually transmitted encrypted on the air interface between mobile devices and base stations. In many cases, the A5 / 1 algorithm is used, which is now insecure. It is thus possible to decrypt the data without access to the key. In many cases where more modern algorithms are used, an attacker can use an active false base station to force the use of the outdated A5 / 1 algorithm or to deactivate encryption altogether.

Even without the use of a false base station, it is possible under certain circumstances to record conversations remotely. To this end, the attacker first causes the mobile network to redirect calls from a particular user to a computer on which the call is recorded. For this, SS7 vulnerabilities are exploited in the infrastructure of the mobile communications provider.

How often false base stations are used unauthorised in Germany is not systematically recorded. Since the costs of such an installation have declined sharply in recent years, a rising trend is expected.

The success of an SS7 attack depends in a particular case on whether the mobile radio operator, in whose network the user has entered, has taken countermeasures. Depending on the mobile operator, therefore, the protection level currently varies. Although more and more mobile operators with SS7 firewalls are addressing this kind of attack during the reporting period, the attack method remains relevant at a global level.

Threats to Industrial Plants

Industrial control systems (ICS) are central elements of our society through their use in critical infrastructures as well as in factory and process automation. Failures or faults usually have serious physical effects, for example, in the form of power failures or production interruptions. The changes in the technologies and infrastructure used in industry 4.0 are continuing to grow. This also applies to the interconnectedness of ICS within companies and beyond company boundaries. Further trends are the integration of cloud services into ICS and the outsourcing of control-specific data and processes into the cloud.

Infections via Malware

Time and again, incidents are discovered in various production systems. Non-targeted attacks are often successful because the company often uses legacy systems over long periods of time, and there are no suitable processes and no know-how for IT security for the production area. On the other hand, manufacturers and machine operators do not receive sufficient information from the providers on the necessary security requirements, as these are neither requested by the operators themselves nor are the corresponding resources intended. In addition, the manufacturers often lack processes to deal with vulnerabilities in their own products, to communicate them, and to provide for an error correction.

In view of the nature of the attacks, ransomware and other malicious software are also a problem in the industrial environment. The malicious software usually enters the ICS mostly via infected USB sticks, maintenance laptops or the corporate network. Since the ICS is often only inadequately protected against malicious software or security updates have not been installed, infection is often easily possible. To make matters worse, security updates can only be installed after approval by the manufacturer or integrator and in the appropriate maintenance windows of the system. Until then, the systems are vulnerable. This problem has also been shown in the context of the ransomware “WannaCry.” Among other things, unpatched ICS, e.g. display panels of Deutsche Bahn were infected and limited in their function.

In 2016, over 120 vulnerabilities were made public in various components or software for industrial applications. In the first six months of 2017 there were already 110.

Exchange between all Parties Involved

Sensitivity to IT security has steadily increased in recent years. However, it is necessary to provide appropriate resources in companies to establish necessary processes to strengthen IT security and to avoid incidents. In particular, the exchange between all parties involved should be mentioned. Security requirements must be communicated to machine operators and manufacturers so that they can take into account and integrate appropriate functions in their products. On the other hand, mechanical engineers and operators are obliged to take IT security into account at an early stage during planning, as well as to observe the instructions and requirements. The same applies to the handling of vulnerabilities by manufacturers. A few manufacturers have established good processes, inform the operators and react quickly to appropriate vulnerabilities reports. This is also necessary for other manufacturers.

In particular, operators of existing plants are required to take organisational and technical measures to protect them. In any case, it is important to avoid connecting these plants to badly secure networks (or even the Internet) without protective measures, as well as exposing them to other risks such as permanent operation without updates or other risk-reducing measures.

DDoS Attack against KrebsOnSecurity

Situation

On 19 September 2016, Octave Klaba from the French web host OVH announced two DDoS attacks via Twitter with the extremely high bandwidths of 1,156 and 622 gigabits per second. The volume of attacks was many times larger than the largest attacks recorded so far by the DDoS mitigation service provider Akamai. On the evening of the following day, the weblog https://krebsonsecurity.com of the security researcher Brian Krebs was hit by a massive DDoS attack of about 620 gigabits per second. In the run-up to the attacks, Brian Krebs had reported critically on providers of so-called booter services, which offer fee-based DDoS attacks against any target.

Cause and Damage

In addition to the size, the attack methods were also striking. Thus, a combination of several types of attacks was registered that had never occurred with DDoS attacks in this form. From a technical point of view, this incident is the first public occurrence of the Mirai botnet. This botnet is mainly composed of IoT devices. In addition to the sheer size of the botnet, several hundred thousand bots, the technical implementation was surprising as well. Mirai is thus able to spread itself independently by searching already infected systems for further vulnerable devices and then compromising them when possible. Therefore, a list of standard identifiers and passwords is used which are set when the devices are delivered. Such systems whose passwords are not changed after delivery can be infected with Mirai quickly. There are also other Mirai variants that exploit weak points in implementations, for example with routers. Successfully acquired systems are integrated into the botnet and deactivate the service through which the device has been compromised. The bot software itself offers new DDoS attack methods such as GRE Flood or DNS Water Torture that achieve a high packet rate through efficient implementation even on low-performing devices.

Reaction

Akamai succeeded in warding off the attack after a few hours of failure. However, since Akamai provided this service in the context of a free, voluntary offer, it was not permanently made available due to the persistent intensity and duration of the attacks as well as the costs involved. Google then agreed to put Krebs's blog under the free protection of Google Project Shield. It has been permanently available since this time.

Recommendation

Due to the free availability of the source code as well as the low technical hurdles to build up a Mirai botnet, Mirai is a massive threat. Implementing effective attack methods allows comparatively efficient attacks with only a few thousand bots. A further complication is the fact that there is a very high number of technically inadequately secured systems worldwide that are accessible via the Internet and which are vulnerable to the exploitation of such attacks. There is an urgent need for action among manufacturers and users of these systems to secure them. According to the findings of the BSI, scanning trials are permanent carried out by Mirai systems and a vulnerable device is successfully infected in less than a minute. In Germany, most of the Internet connections of private customers are placed behind routers. It is therefore important to configure the router, the link between the Internet and the home network in such a way that it is not possible to penetrate connected devices in the home network or that the connected devices do not receive a direct approval for communication over the Internet.

Distributed Denial of Service (DDoS)

In 2016, media was filled with reports on distributed denial-of-service attacks. In particular, the botnet Mirai was widely perceived in public. In this context, the attacks on the blog of the journalist Brian Krebs, the attack on the DNS service provider Dyn and the attack on the host OVH (see info box DDoS).

Attacks in the three-digit gigabit or even terabit range are a serious threat. At the same time, however, these attacks are also exceptional phenomena. In the first quarter of 2017, the BSI is aware of two attacks in Germany that were beyond 100Gbps. This corresponds to 0.005 percent of the attacks known to the BSI. Most of the DDoS attacks still have a bandwidth of less than one Gbps (see figure 11). While the maximum deviations for bandwidth, packet rate and duration vary widely, the average values are largely constant.

Media reports often address attacks with high bandwidths. However, the bandwidth alone is not a suitable indicator of the severity of an attack. With upstream components such as load balancers or firewalls, the limiting factor is often the number of packets that can be processed. Attacks on application levels, such as TCP connections or HTTPS requests, can cause significant damage, even with low bandwidth and low packet rates. Essential elements of effective protection against DDoS attacks are not only technical possibilities but also organisational measures. The BSI has published corresponding cyber security recommendations.

Vulnerabilities in Hardware

Kerckhoff's principle states that an encryption algorithm must not depend on the secrecy of the method itself, but on the secrecy of the key. Modern cryptographic procedures are an example of this basic principle. For them it can be shown that it requires the solution of a mathematical problem, which is regarded as a difficult one, to break the process.

However, a problem remains to store the key and process it unseen. In this case, hardware security elements are often used which compulsorily use the controversial principle of security through obscurity in order to keep the stored keys secret. This takes place, for example,

- by the operations performed being obscured by software,
- by cryptographic blinding,
- by means of physically implemented measures such as a sophisticated sensor system, which constantly monitors the operating conditions and detects attacks,
- or even by the small structural size prevailing in today's chips.

All these measures can be the target of an attack. Invasive attacks on the hardware in which physical manipulations are carried out on the chip, for example, by means of

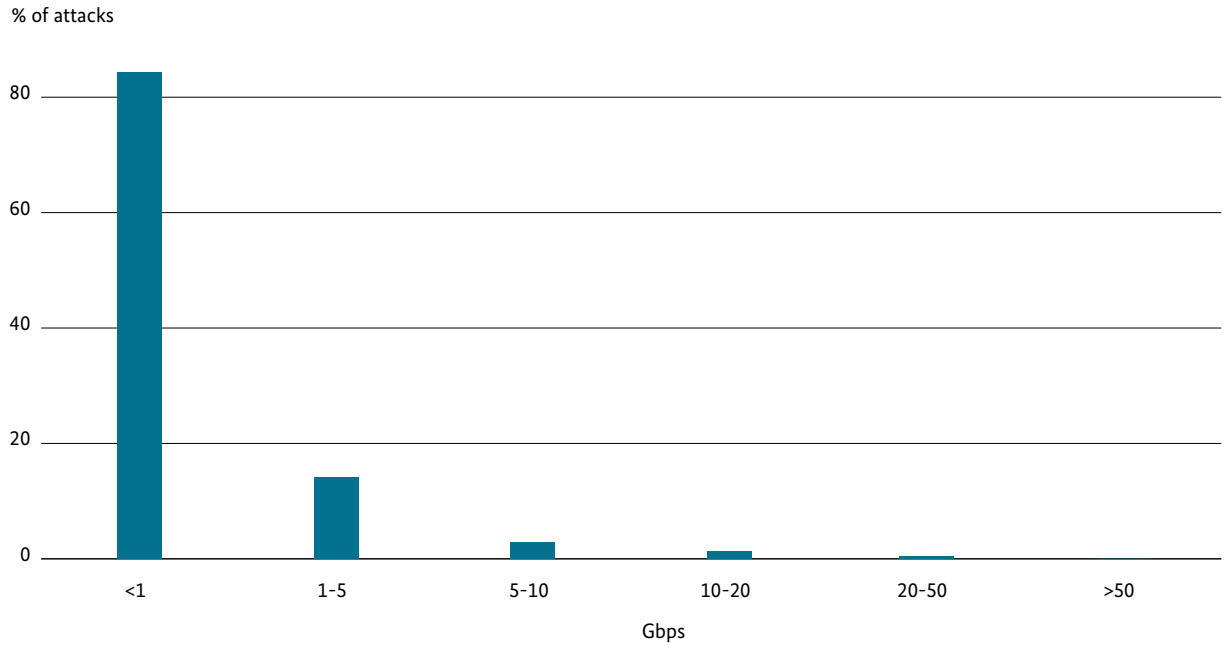


Figure 11 Distribution of DDoS attacks by bandwidth in the first quarter of 2017

fault induction attacks by laser bombardment up to the modification of the circuits, are not widely used due to the effort required. Side-channel attacks, however, are gaining in importance. Since high-resolution oscilloscopes are relatively inexpensive in the market or in research facilities, the measurement of local electromagnetic emission, for example, of a crypto-coprocessor is no longer a great challenge. Even with side-channel-resistant implementations, conclusions can be drawn about the processed key material over time by improved analytical methods. In recent years, have also been utilised physical effects which have not been considered so far for new side-channel interventions, e.g. photon emissions of semiconductors. Due to the partly very different underlying physical effects, new countermeasures must always be developed in order to prevent these effects from being exploited for side-channel attacks.

By combining improved measurement methods for observable physical effects on the one hand and specialised mathematical evaluation methods of these measured values on the other hand, the cryptographic keys can already be extracted with a relatively small number of measurements in the case of inadequate countermeasures.

Since side-channel attacks are continually optimised, they are a threat to security elements in practice with the growing age of the hardware, even if their security was originally successfully certified according to common criteria. For this reason, the validity of the security certificates is limited, for chip cards and similar products usually to five years. For security-relevant applications, which are in the field for a longer time, update mechanisms should be provided at least for the implementation of the cryptographic methods. In this way, additional countermeasures can be taken in software to prevent new attacks that use improved analytical methods at an early stage.

Vulnerabilities in Web Applications

Almost every authority, institution and company provides information or services through web applications on the Internet. Vulnerabilities in these web applications can have considerable negative consequences for the provider as well as for the user. These range from damage to the company's image to the theft of sensitive data.

To find as many as possible of such vulnerabilities before the publication, the BSI offers so-called IS web checks. These are penetration tests on web applications that are specifically searched for known vulnerabilities in web applications and the web server configuration. The vulnerabilities found are divided into three categories:

- Critical deficiencies – include, for example, the risk that data will be changed or vendor systems are penetrated
- Serious deficiencies – describe possible configuration errors that can result in serious attacks
- Other deficiencies – are present, for example, with configuration errors with undefined attack potential.

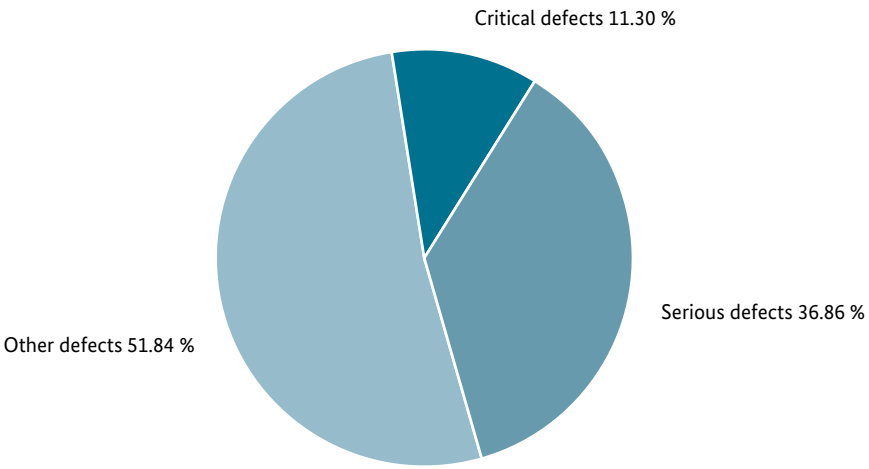


Figure 12 Defects detected in web applications by category

Vulnerabilities in Content Management Systems

Situation
In April 2017, an incident occurred in a company where attackers were gaining unauthorised access to the web server on which the content management system (CMS) was installed by exploiting a vulnerability in an outdated plug-in version for a CMS. By using a so-called reverse shell, the attackers could then access and delete the data from another CMS installed on this server. In addition, the perpetrators were given access to a backup server and also deleted the data backups of the content management systems stored there. At the end of January 2017, the manufacturer released an update for the CMS that closed a critical security breach. Already in the first days after the update was released, attackers exploited these vulnerabilities in CMS installations that have not yet been updated to manipulate tens of thousands of sites.

Cause and Damage
CMSs offer comfortable ways to create and maintain websites. Like other software, they are not free from errors and must be maintained regularly. However, many operators are very sloppy and do not or only with a long delay implement updates, which close, among other things, vulnerabilities. According to an analysis by BleepingComputer, more than 60 percent of the examined installations of the popular CMS "WordPress" were not up-to-date in the third quarter of 2016, and of "Joomla" even more than 80 percent. In addition to the CMS itself, installed plug-ins must also be kept up-to-date. This is often neglected by CMS operators and can therefore be exploited by attackers as a gateway for attack. The compromised websites are then misused, among other things, for spreading malware, manipulating the results of search engines (BlackHat-SEO) or sending spam. There are also regularly taking place so-called "defacements" for spreading political messages.

Reaction
CMSs are usually accessible from the Internet and are therefore often the focus of attackers. Cyber criminals exploit known vulnerabilities daily in outdated versions of current CMSs to compromise large-scale related websites (automated). In the present case, the non-maintained CMS was only used as a gateway for the attack on the actual target. The primary CMS was protected on the current patch level and by a secure password.

Recommendation
The incident illustrates once again that software installed on servers accessible via the Internet, including older and possibly no longer used ones, must be regularly updated. What is important here is that not only the basic CMS needs to be updated, but also all installed plug-ins, which often have no automatic update functions.

The assessment takes into account the protection required by the data to be processed. The classification is also estimated using the skills and means required for an attack.

In the period from March 2016 to March 2017, 63 IS web checks were carried out by the BSI on web applications. The tests were carried out on a sample-by-sample basis and mainly on websites of government authorities in a mixture of tests before commissioning and repetitive tests (see figure 12).

Repeated tests found more severe and deficient defects, while critical deficiencies were mainly found in initial tests. It was striking that in the area of critical deficiencies, vulnerabilities were still found, such as cross-site scripting or SQL injection known for years, which are based on an insufficient input validation. In the area of the serious deficiencies, configuration weaknesses were often found with SSL encryption. As other deficiencies, mostly missing HTTP headers were detected, which increase the security during the transmission and storage of the data. The minimum standards and recommendations of the BSI provide a remedy.

Spam and Malware Spam

Unwanted sent e-mails are generally referred to as spam. This can be divided into three forms:

- Classic spam is often used for product, securities or service advertising, and is also used for fraud attempts such as advance fraud.
- With malware spam, attackers want to infect systems of the receiver with malware. This can be done directly by malware in the e-mail attachment or indirectly by a link in the e-mail text or in the attachment, which refers to a malicious program or a website with drive-by exploits.
- With phishing messages, users are encouraged to enter their access data (for example, to Internet banking, payment services, social networks, shopping portals, etc.) on websites under the control of the attacker.

In most cases, spam is dispatched either through compromised servers, infected client systems or via spoofed access data through legitimate e-mail accounts. Frequently, the spam-sending systems are integrated into a botnet, which facilitates the marketing of spam as a service by cyber-criminals.

The use of personal data from data leaks with large service providers or even researched data is currently being observed more and more frequently. This greatly increases the likelihood of infection.

Necurs Dominates the Spam Landscape

With a size of about five million bots, Necurs was one of the largest known botnets in 2016. It was responsible for most of the malware spam messages sent in 2016 and distributed downloaders of the crypto-ransomware Locky and Cerber until December. Before 16 February 2016 – the "birthday" of Locky – it was mainly downloaders for the banking trojan Dridex.

Usually, the downloaders were sent as (zipped) scripts in the attachment, which are executed by default under Windows by the Windows Scripting Host. MS Office documents with downloader macros in the attachment were somewhat less frequent. Separated campaigns completely forgo a download and delivered the malicious software coded embedded in the script, document or macro.

After Christmas, the dispatch of such malware waves was discontinued. What initially looked like the Necurs Christmas break, which had already been observed at the beginning of 2016, seems to have been a strategy or customer change. Since April 2017, there has been recorded an again increase in malware spam. However, the largest daily volumes observed up to 30 June 2017 were about 10 times smaller than before Christmas. The attack methods vary widely. Thus, e.g. a Microsoft Word vulnerability (CVE-2017-0199) was exploited already one day before the release of patches in attached RTF files. Also, different embeddings of the malicious files, e.g. in PDF documents are observed.

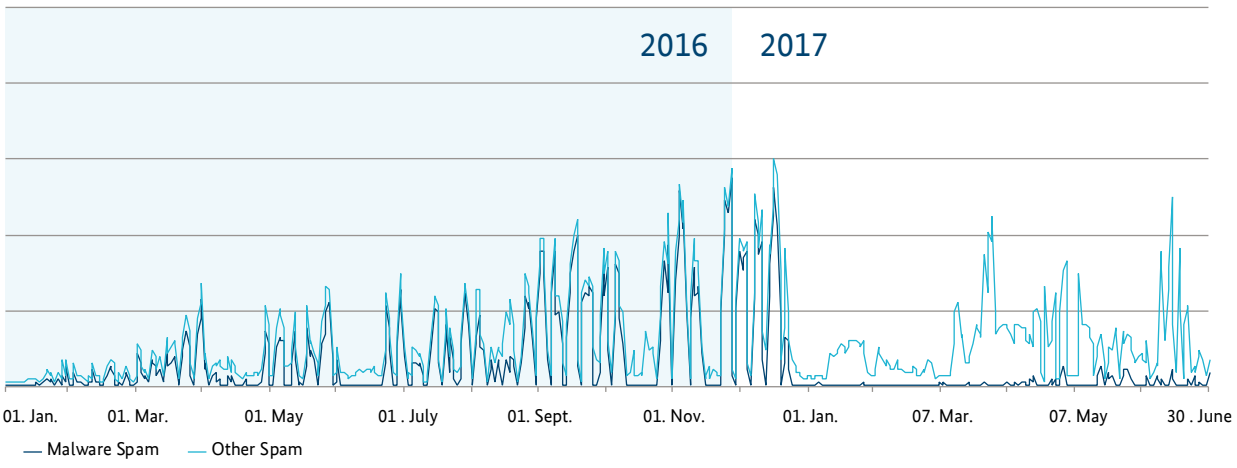


Figure 13 Qualitative history of classic spam and malware spam

The first major Necurs waves after the long pause were observed at the end of March 2017. These sent a so-called pump'n'dump campaign with an alleged insider tip to a so-called Penny share and led in the short term to the extreme increase of the trade volume and a moderate increase of the share price. The campaign appears to have been unsuccessful for the perpetrators, as they continued after the short-term price rise on the first day, with the share price continuing at a consistently low level. Further similar campaigns with a minor impact on the price movements of the affected shares were also observed afterwards.

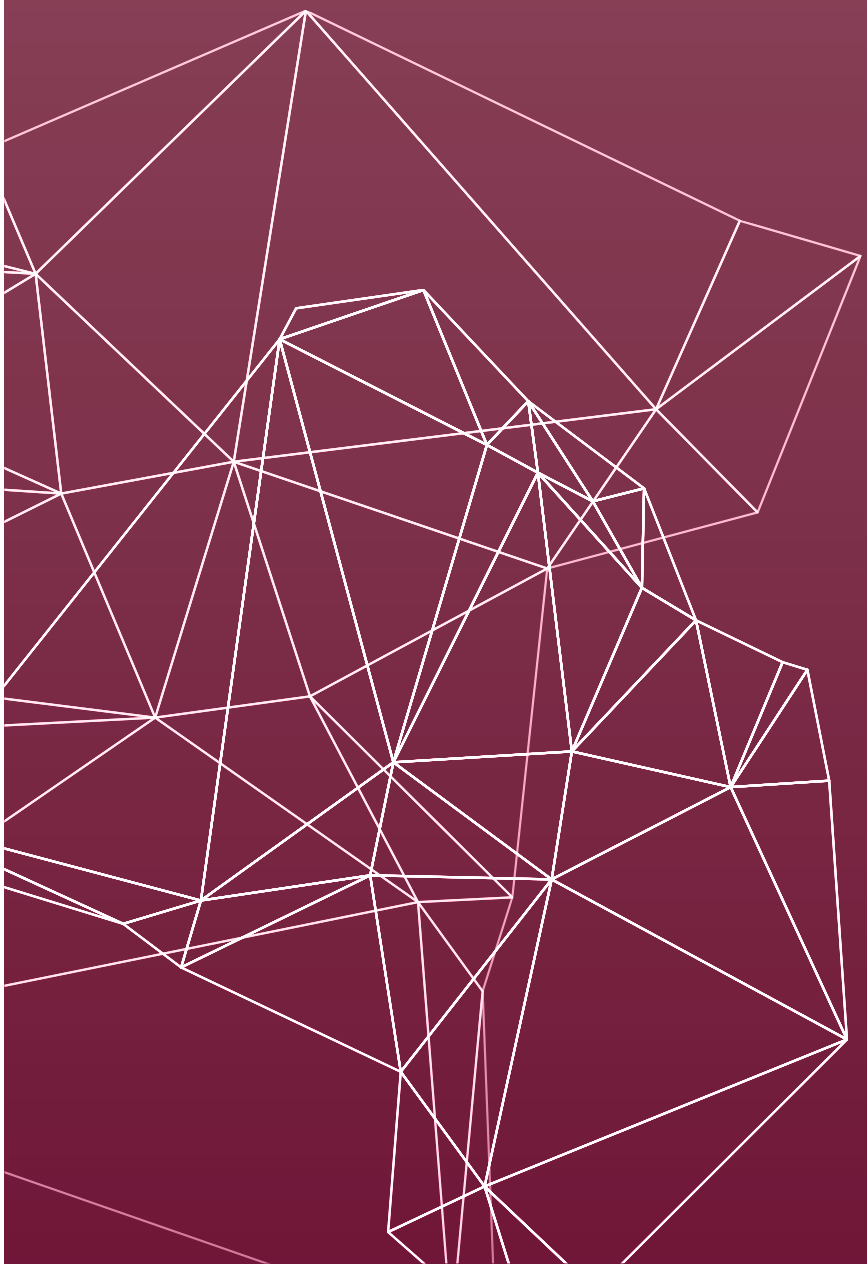
At present, Necurs appears to be used with less than 30 percent of its capacity for shipping advertising for binary options trading. As the BSI was able to verify, the current versions of Necurs also have a DDoS component since September 2016, but they have not been used prominently so far. If the operators do not reach "infrastructure utilisation" with spam, it is conceivable that the DDoS functionality is monetarised.

Small Malware Spam Campaigns Continue to Run

Independent of the Necurs network, significantly smaller malware spam campaigns are still being observed. Particularly noteworthy are the recurring spam waves, which address the addressees personally in German language and contain their full address and telephone number. The topics vary greatly. Used are alleged invoices, package preparation attempts, credit notes etc. The purpose of the senders was mostly the installation of malicious software, especially the Crypto-ransomware Cerber. According to the BSI present evidence, the data originate from the eBay hack from the beginning of 2014.

Even more elaborate was the dispatch of alleged applications to companies. Here, personal contact data from staff of the HR departments were researched and used for personal salutations in the e-mail as well as in the attached document (see info box ransomware in HR departments page 28). The document contained only partially legible application documents with a photo. The unreadable / cryptic part should allow the recipient to allow macros in the document. After activating macros, the Crypto-ransomware Petya / Mischa or its variant GoldenEye was started.

2 Shaping Cyber Security



2 Shaping Cyber Security

How does the BSI deal with these threats and what measures can be implemented to counteract them? The following section presents solution approaches and offers by the BSI on the basis of selected topics and always related to the current vulnerability situation of IT security. It is divided into the three areas of responsibility: state / administration, business / critical infrastructures and society / citizens. In order to make these offers practically usable, links to numerous publications and Internet offers of the BSI are referred to.

2.1 Tasks and Structure of the BSI

The BSI as the national cyber security authority shapes information security in digitalisation through prevention, detection and reaction for government, business and society. For this reason, the BSI has a clear legal mandate, which was once again significantly expanded in the field of critical infrastructures by the IT Security Act in 2015 and in 2017 with the implementation of the NIS Directive in the area of digital service providers. The BSI implements this mandate with a strong cooperative approach. As the centre of excellence for questions of IT and cyber security, IT security analyses, the elaboration of technical guidelines, the solution of practical IT security problems and the professional discourse with experts from industry, specialist organisations and associations are among the main fields of action of the BSI. All the necessary competences for coping with highly complex questions are combined in the BSI, from cryptography, network and system, for example, up to chip security. This bundling and networking of all competences required for cyber security in one authority gives the BSI its unique impact in Germany.

With the allocation of 180 new positions for 2017 alone, the role of the BSI as the national cyber security authority was further strengthened. The agency has thus grown to around 840 employees. In order to fill the 180 new positions, the BSI has launched a personnel recruiting campaign. Despite the hard-fought labour market for IT specialists, the BSI, as a top employer for IT graduates (trendence Graduate Barometer), was already able to fill 60% of these positions in the first half of 2017 (as of June 2017).

The BSI also takes account of changed requirements through reorganisation.

The change in the structure of the agency with its four specialist departments, which are supported by the central department, is at the same time a reflection of the guiding principle of the BSI.

- In division CK "Cyber Security and Critical Infrastructures," all topics of cyber security are bundled and shaped.
- In division B "Consulting for Government, the Private Sector and Society" all consultancy tasks are bundled within the scope of prevention.
- The division KT "Cryptotechnology and IT Management for Increased Security Requirements" bundles on the one hand all tasks in the area of specification and approval of cryptographic systems, and is, on the other hand, responsible for their evaluation and operation.
- Cyber security in digitalisation is a growing focus of division D "Cyber Security for Digitalisation, Certification and Standardisation."
- The central division Z "Central Tasks" supports the above-mentioned departments by internal services.

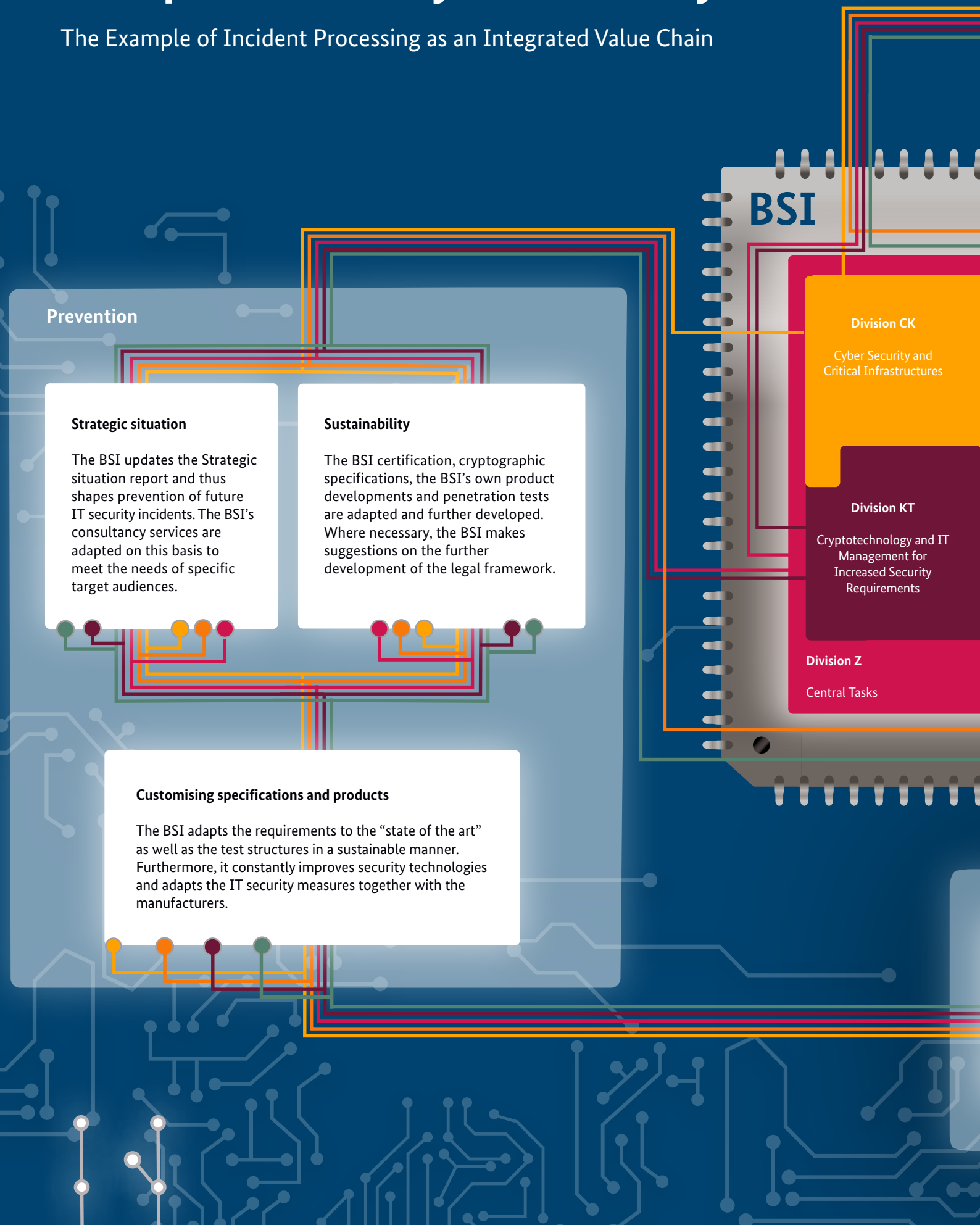
2.2 Target Audience State / Administration

2.2.1 The National Cyber Response Centre

The National Cyber Response Centre is operated under the leadership of the BSI on the basis of administrative agreements between the authorities involved. The BSI provides the director, the office, the staff and the premises. Through the establishment at the BSI, the Cyber Response Centre can work closely with the National IT Situation Centre / IT Crisis Reaction Centre, the CERT team and the MIRTs (mobile incident response teams) of the BSI. The other authorities involved are linked through the liaison officers of these authorities.

The BSI – Networked Competence in Cyber Security

The Example of Incident Processing as an Integrated Value Chain



Detection

Detection of the vulnerability

The BSI carries out tests of the hard- and software, covering vulnerabilities. These vulnerabilities are evaluated and security analysis are performed.

Recognising an attack

The BSI detects anomalies in IT networks and systems and thus identifies actual cyber attacks.

Division B

Consulting for Government, the Private Sector and Society

Division D

Cyber Security for Digitalisation, Certification and Standardisation

Reaction

Coordination of cyber defence

The BSI, as the national IT crisis reaction centre, coordinates efforts by the contacts to manufacturers, providers, stakeholders, the IT security industry, critical infrastructures and other authorities.

Combatting a cyber attack

The BSI supports the affected institutions with defending against concrete attack and helps to restore normal operations. The government, the business, society and international partners are informed of all necessary measures.

Evaluation of a cyber attack

The BSI, in cooperation with all other expert areas, prepares a presentation of the situation and assesses the incident, the vulnerability and how it has been taken advantage of. This exploitability is broken down again based on deployment scenarios for the government, business and society.

In addition to the exchange of cyber-relevant information, the work of the Cyber Response Centre is aimed in particular at coordinating the handling of cyber incidents in Germany and matches the operational measures of the responsible authorities. Much of the case processing is undertaken by the authorities concerned, such as the Federal Office for the Protection of the Constitution, the Federal Criminal Police Office, the Federal Intelligence Services, the German Armed Forces or the Federal Office of Civil Protection and Disaster Assistance as part of their respective tasks by their divisions. In doing so, the results are continually merged in the Cyber Response Centre, evaluated and reported to the relevant authorities. In this respect, the Cyber Response Centre can access human resources of all authorities involved. They are currently being strengthened at all Cyber Response Centre authorities.

The Cyber Response Centre is designed as a cooperative platform. The Head of Cyber Response Centre has no direct power of attorney to the authorities involved in the Cyber Response Centre or their employees. At present, the authorities involved are developing a concept under the leadership of the Federal Ministry of the Interior, with which the Cyber Response Centre will be further developed.

2.2.2 Cooperation between Federal Government and Federal States and Liaison Offices

Digitalisation is a global society challenge. The Federal Government and the Federal States are jointly developing the digital transformation in German Federal and State Authorities.

Together for More Cyber Security in Germany

Pursuant to the BSI Act, the BSI advises the Federal States at their request and develops together with them joint IT security standards in the bodies of the IT Planning Council. The BSI's cooperation and support offerings for the Federal States are diverse. They range from the provision of demand-oriented information and general advisory and committee work to the integration of the Federal States into the information and warning channels of the BSI. Further points of action and pillars of cooperation are

- the provision of established BSI security solutions for use by the Federal States,
- the sharing of experience in the establishment and operation of an information security management system (ISMS) as well as technical protection mechanisms,
- the provision of adapted work aids on the security advisory portal,
- the use of trustworthy IT security providers, certified by the BSI,
- the support of the Federal States in IT security incidents by mobile incident response teams (MIRT) of the BSI,
- consulting and support for IT security within the framework of Federal States elections.

Central Contact Point

The BSI's information security consulting is the central point of contact primarily for the information security officers of the Federal Administration on all aspects of information security. Together with the sections of the BSI, security consulting offers both accompanying support and individual advice on specific challenges. The goal and motivation is to provide the customer with knowledge about information security and to find practice-oriented solutions together. In order to make workflows and information channels efficient, the proven point-of-contact principle is applied between the BSI security consulting and the ISMS team of the authority. The security consulting provides a central BSI contact partner for each Federal Authority. In addition to the central e-mail address Sicherheitsberatung@bsi.bund.de and the possibility of direct contact with the consultant, personal advice and on-site appointments are also offered to the authorities. This is often the case in the form of talks in which BSI specialists are also involved on specific subject areas. The accompanying committee work, in which the information security consulting provides aspects of information security and supports in moderation, is also part of the task spectrum.

At the heart of the cooperation between the BSI and the Federal States is the AG InfoSic (working group information security) of the IT Planning Council. This working group coordinates cooperation between the Federal Administration and the Federal States in terms of information security. Each Federal State is represented by a person responsible for IT security (CISO). The German Rural District Association (Landkreisstag) and German Association of Cities (Städtetag) are also represented. In the AG InfoSic, all questions of information security will be addressed as a matter of principle which concern the Federal Administration and the Federal States.

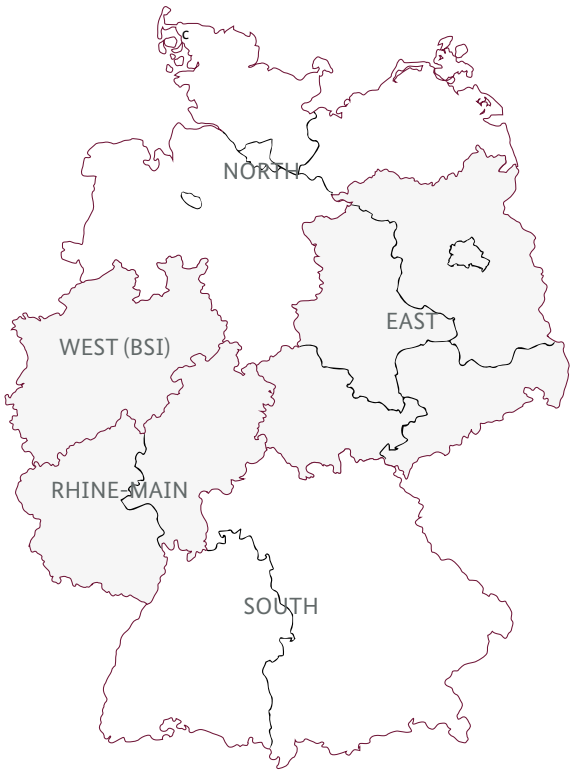


Figure 14 Planned implementation of the national liaison offices of the BSI

One of the most important topics is the establishment of ISMS structures in Federal States and municipalities. In 2016, the BSI began to expand the range of services offered to the Federal States.

In addition, the cyber security strategy for Germany 2016 calls for even closer cooperation between the Federal Government and the Federal States in the field of cyber security. This includes additional tasks for the BSI, particularly within the framework of the support of the Federal States, which the BSI is able to fulfil, among other things, through the expansion of the liaison offices. The BSI is becoming more accessible to Federal States, Federal Agencies, international organisations and the economy in key regions by sending out contact persons to different national and international locations. The liaison officers locally provide information on the products and services of the BSI in order to better meet the needs of users in the fields of government, business and society. The regional locations in the Rhine-Main area, Berlin and Brussels are the focus of the expansion of the communication system. Representatives of the BSI in Southern and Northern Germany are to follow.

2.2.3 Counter Eavesdropping

The BSI provides counter eavesdropping concepts and services to Federal Authorities that are susceptible to interception. This includes

- publication of technical guidelines,
- consultation on new and reconstruction measures as well as
- conducting of initial and repeat counter eavesdropping audits.

The BSI also offers configuration tests for telecommunication systems. This involves the settings of the systems being analysed using a test tool developed by the BSI. Subsequently, the BSI advises the relevant authority which measures are necessary to secure their telecommunication systems.

In addition, such as the G20 Foreign Ministers' Meeting in Bonn in April 2017, the G20 summit in Hamburg in July and bilateral meetings at a higher level, with which the confidentiality of the discussions is of particular relevance. At the same time, the BSI's counter eavesdropping teams ensure that no bugging devices are present and that no discussed information can reach unauthorised parties in other ways, for example via manipulated or inadvertently activated mobile phones.

2.2.4 Secure Mobile Communication

For processing and transmission of classified information, the BSI provides various mobile solutions for the Federal Administration. The SecuSUITE solution from Secusmart has been established for several years. In the current reporting period, the user numbers of this solution have further increased, so that approximately 15,000 mobile devices are now in use in the Federal Administration.

App Testing

The mobile solutions developed for the Federal Administration are evaluated by the BSI in the field of safety with the aim of approval for the processing and transmission of classified information. The apps used are also checked for security. The BSI has defined criteria for assessing app security, according to which specialised vendors submit the apps to different testing procedures. Since 2014, the BSI has tested around 300 apps for the operating systems Android, Apple iOS and BlackBerry OS on the basis of various criteria such as access to calendars and address books, location data and the use of tracking

mechanisms. The range of the security deficiencies detected is large. While some apps violate only a few criteria, other apps have significant deficiencies, such as handling of user data. To enable more sophisticated risk management, the BSI submits the test reports to post-processing, where the various criteria are weighted according to the application. The test reports are made available to the Federal Administration, which can make a well-founded decision on this basis about the use of the respective app in their respective area of responsibility.

iOS System Solution

The iOS system solution is a solution designed by the BSI to be able to process classified data on iPhones and iPads from the manufacturer Apple. The main feature of the solution is the "SecurePIM Government SDS" app from Virtual Solution AG. This app combines e-mail, address book, notes, tasks and calendars, and allows synchronisation of this data with the network's internal network. In addition, documents and other content can be downloaded from the Intranet to the mobile devices. As a security anchor for SecurePIM Government SDS, the solution uses a chip card, which is coupled to the iOS devices via special smartcard readers. In addition, an IPsec VPN as well as Mobile Device Management (MDM) are used for the communication link to the authorities' network. During the reporting period, the system was put into operation in more than 20 authorities under a pilot project and approved by the BSI after a safety assessment.

SecuTABLET

The mobile solution SecuTABLET from Secusmart uses Android tablets from Samsung for secure processing of official data and their synchronisation with the network within the authorities. Therefore, security technologies such as Samsung Knox and Secusmart's wrapping technology are linked to ensure the security of the data. The mobile solution uses a chip card as a security anchor in the devices, uses IPsec VPN for the communication connection to the authorities' network, and manages applications and devices via the on-premise mobile application management (MAM) server. This separates business and personal applications on the end devices. In the back end of the authorities' network, different PIM data servers can be contacted. During the period under review, the solution was delivered to official users for the first time after a preliminary approval of the BSI.

2.2.5 Development of IT Systems for the Processing of Classified Information

IT systems that are used to process or transmit information requiring confidentiality (classified information) in the public interest must be approved by the BSI. The relevant Classified Information Directive (VSA) from the Federal Ministry of the Interior on the physical and organisational protection of classified information regulates, among other things, when approved IT systems have to be used and how these are to be handled correctly. The VSA also provides guidance

5G Increases IT Security Risks

The 5th generation of mobile technology (5G) enables a range of numerous innovative applications and combines previously independent areas. An average household will be equipped with a variety of devices which communicate with each other, cars will be able to exchange various types of data with each other, as well as with traffic-infrastructure assets. Office communication and production processes will also be pervaded by 5G technology. The risks of IT security will not simply increase in proportion to the number of communicating devices and components in the 5G era. The factor of general networking, the increasing complexity of the overall systems as well as the gradual transfer of critical tasks to the 5G technology will lead rather to an increase in the security risks.

The opportunities offered by digitalisation can only be exploited if the risks become manageable. In this sense, IT security needs should be adequately taken into account from the outset – in standardization, production and operation. Successful use of 5G requires all stakeholders to take IT security concerns into consideration from the outset, in standardisation, in production and in operation. Safety is an indispensable prerequisite for the success of the entire 5G technology. The task of the BSI is to shape this core issue of digitalisation with its challenging security problems in its opportunities and risks. The BSI is well prepared for this new challenge due to its technical and scientific competence and its high degree of networking in all areas of state, business and society.

Challenges of Globalized Production Processes

A guideline of the cyber security strategy for Germany adopted by the Federal Government states that the ability to act and the sovereignty of Germany must also be preserved in the age of digitalisation. However, most IT products or their components are no longer manufactured in Germany or the EU. If one has no control over the manufacturing process or the supply chains, manipulations on the finished IT system cannot be ruled out. That this is not an abstract threat scenario is shown by several current cases in which factory-installed malware has been found on large production volumes of Android devices.

The BSI responds to this challenge with various measures to enable and promote trustworthy manufacturing processes. For example, cooperation agreements are concluded with manufacturers in order to gain insight into the exact structure or source code of IT products. A further possibility is that the BSI performs its own development of the required product or of partial components. This is done through invitations to tender, which companies can apply for who are prepared to meet the requirements of the BSI with regard to the greatest possible transparency of the development, production and delivery processes. If there is no alternative to the use of non-trustworthy subcomponents in a VS-IT system, there is still the possibility to reduce the remaining risk to an acceptable level by means of a suitable conception of the overall system. This can be achieved, for example, by isolating the non-trustworthy components so strongly from the rest of the system that they cannot cause any harm.

on the security functionality that IT systems must have in order to be approved for a certain classification level. The VSA, for example, requires that classification level for processing of classified information with the level CONFIDENTIAL or higher technical or organisational measures must be taken so that unauthorised parties cannot obtain secrets by intercepting compromising emissions.

As a legal standard, however, the VSA cannot cover every conceivable situation or be adapted to new technologies or threats at short notice. It is therefore the responsibility of the BSI to formulate concrete security requirements for VS-IT systems. On the one hand, an interpretation of the VSA is necessary in order to derive concrete requirements for the individual case from abstract legal norms. On the other hand, the BSI must constantly check and adapt the security requirements to VS-IT systems to meet technological progress as well as emerging threats. The balancing act between security functionality and user acceptance must also be overcome, as users from the field of government and business expect also for processing of classified information modern, affordable, mobile and easy-to-use solutions, as they are accustomed from market-oriented products.

Already during the conceptual phase of VS-IT systems, the BSI works closely together with manufacturers and stakeholders to define the security requirements and record them in the so-called security target. During the development process, the BSI then checks within the scope of the development-accompanying evaluation whether the manufacturer has implemented the requirements from the security target effectively and correctly in the product. Where appropriate, technical and organisational advice on the use is formulated, which must be observed by the stakeholders. If all requirements are met, the BSI will issue a national approval for the VS-IT system. In order to enable the product to be used in the international context (EU, NATO, etc.) and thus to significantly increase the market opportunities of the product, international requirements must be considered in addition to national requirements.

2.2.6 Federal Administration IT Consolidation

On 20 May 2015, the Federal Government decided to consolidate the IT of the Federal Administration. This includes

- to gradually concentrate the IT operation of the direct Federal Administration by 2022 on one or two service providers in a few locations (operational consolidation),
- to summarize the development of applications often required by the Federal Administration and to build up a “Federal Cloud” (application consolidation) as well as
- to merge IT procurement in a few places in the Federal Administration (procurement bundling).

For this purpose, the Federal Government has set up a cross-departmental project consisting of six sub-projects. It is managed by the Federal Commissioner for IT in the Federal Ministry of the Interior.

One of the project objectives of IT consolidation is

to maintain the level of IT security of the Federal Administration. The BSI advises the Federal Government on security aspects in the implementation of operational and application consolidation.

Operational and application consolidation can bring a gain of IT security if IT security is a priority from the outset. The sustainable maintenance of the IT security level also requires the planning and implementation of appropriate security measures. As part of its advisory activities, the BSI regularly updates the various stakeholders on safety requirements. To develop appropriate security concepts for common IT systems is the responsibility of the IT service providers in the service network.

In addition to IT consolidation, the budget committee of the German Bundestag has commissioned the BSI to analyse the level of IT security of all Federal Government data centres. The BSI fulfils this mandate by successively examining all centres on the basis of the standard "HV benchmark" assessment scheme and reporting the results to the budget committee.

2.2.7 Other Measures for the State

Portal of Information Security Consulting for Federal Administration and Federal States

The BSI's information security consulting is mainly provided by the direct contact between BSI consultants and experts and the ISMS team of an institution (see 2.1.2). In addition to the personal contact, all essential information is always available on the BSI website and in the web portal for the information security consulting of the BSI. The web portal provides the general information of the BSI in an open area. In addition, target audience-specific information is also made available in an internal area.

- In the open area, for example, work aids are provided such as a conceptualisation and evaluation tools for surveys and information on penetration tests and IS revisions, dates and events on training courses, as well as the list of approved IT security products and systems.

- In the internal area "Federal Administration," the BSI's products, services and publications for the Federal Administration target audience are provided. Among other things, there are IT security warnings, safety notes, BSI documents and status reports. Official information, orientation papers on current topics such as framework contracts, emergency management and awareness raising round off the offer.

- In the internal area "Federal States / Municipalities," the products, services and publications of the BSI for the target audience of the Federal States / Municipalities are published. Here can be found, among other things, blueprints for the development of an information security management system (ISMS), the implementation framework for emergency management as well as the technical guidelines for the BSI (BSI-TR) and VSA (BSI-TL).

Minimum Standards

In accordance with § 8 BSIG, the BSI establishes minimum standards for the Federal Government bodies and thus provides a targeted minimum level for the information technology of the Federal Administration. The first published standard on the use of the SSL/TLS protocol by Federal Government authorities was issued by the Federal Ministry of the Interior in agreement with the IT Council as a general administrative regulation. Thus, the Federal Administration is obliged to encrypt all data traffic over unprotected networks using SSL/TLS. Over the last year, the minimum standards of secure web browsers, interface control, use of external cloud services, mobile device management and application of the HV benchmark assessment scheme have also been published. Further minimum standards from the fields of network security and detection are currently being developed.

Examination Samsung Knox

Mobile devices with the Android operating system are also very popular in the Federal Administration. In the professional environment, however, the requirements for security and the possibilities to manage the devices and applications are higher than those for the private user. With the Samsung Knox solution, the mobile device manufacturer Samsung is addressing this area and providing advanced security features that go beyond the features provided by Android. In addition to the verification of system integrity and an additional data separation using the so-called Knox containers on the end devices, Samsung Knox also offers additional possibilities of the end-device management.

The BSI examined this solution in 2016 and included the findings in the evaluation of Android-based mobile solutions for Federal Administration (like SecuTABLET, see 2.2.4 Secure mobile communication). For administrators in authorities and the business world who already use or plan to use Samsung Knox, the BSI has published configuration recommendations on its website. It shows possible approaches to secure and configure Android-based mobile solutions using the Knox functions. In addition, the BSI provides concrete

safety recommendations for the variety of configuration options. Based on two exemplary mobile device management systems (MDMs), useful configuration parameters for Knox devices are presented from the security perspective.

Like most complex IT systems, Samsung Knox is also not free of security vulnerabilities. In addition to the Android vulnerabilities that Google regularly publishes and closes with security updates, security researchers reported vulnerabilities twice in the reporting period that enabled immediate attacks on security features from Samsung Knox. Both publications show ways to bypass the real-time protection for the operating system core. In the spirit of responsible disclosure, these weak spots were reported to the manufacturer before their release, and were corrected by Samsung in some models. However, this also shows the problem known from the Android environment that not all vulnerabilities are addressed quickly on all devices and on some devices not at all.

Approval

The BSI is legally authorised to examine IT security products and to make binding statements about security value. In particular, IT security products used for the processing, transmission and storage of officially classified information at the Federal Administration and the Federal State Authorities or companies as part of orders from the Federal Administration and the Federal State Authorities require this evaluation and approval by the BSI. This applies mainly to IT security products that contain cryptographic components and are therefore referred to as cryptosystems. The application for approval for an IT security product can in principle only be submitted by a governmental user.

According to Section 37 of the Classified Information Directive (VSA) from the Federal Ministry of the Interior, approval must be provided by the BSI for products used to create encryption, for encryption itself, for securing transmission lines and for separating networks with differing maximum classification levels for the classified documents to be processed. Over the reporting period of July 2016 to June 2017, the BSI issued or extended 59 approvals for this purpose. 46 approvals were withdrawn or replaced by approvals of newer versions. BSI Document 7164, which is available on the BSI website, can be referred to for an updated list of approved IT security products.

Optimisation of the Approval Process

At present, the BSI is currently dealing with more than 60 ongoing procedures seeking approval. In order to accommodate the rising demand of the (Federal) Administration for approved products and secure IT solutions, the BSI will optimise the approval process and significantly increase the development and provision of VS requirements profiles (VS-AP). VS requirements profiles describe IT security requirements for specific product classes and types. On the one hand, they are directed at users and operators, such as authorities who want to use products when dealing with classified documents, and who need the basic requirements that must be met by suitable products. On the other hand, VS-APs are aimed at manufacturers of such products in order to give them a general technical guideline for the implementation of relevant IT security requirements.

The following objectives are pursued in optimising the approval process:

I. Forward-looking design of information-assuring systems and components for the VS area by the BSI

II. Harmonise IT security requirements for certain product classes and types

III. Appropriate determination of requirements by directly involving users, operators and product manufacturers in the design of corresponding VS-APs

IV. Efficiency enhancement of the approval process in the BSI by early provision of relevant VS-APs

Currently, the BSI has published three VS requirements profiles. A further eight VS-APs are currently being created. As a result, the BSI already covers the widest range of products for the protection and processing of classified information. Parallel to this, a large number of VS-APs and national protection profiles (nPP) are being prepared for use in the VS area for the standardisation of further IT security products. The decision to involve product manufacturers, users and operators at an early stage in the design of such IT security requirements led to a consistently positive response in the reporting period, as well as strong participation in the described procedure.

Outdated Cloud Software

Situation

In February 2017, the BSI experienced several tens of thousands of the private cloud systems operating in Germany, based on the widely used software ownCloud and Nextcloud, were running with outdated versions that were no longer supported by the manufacturers and had in part critical vulnerabilities. Among the operators of these vulnerable cloud systems were, among other private users, many large and medium-sized companies, public and municipal institutions, energy suppliers, hospitals, doctors and lawyers.

Cause and Damage

Updates provided by the manufacturers of the cloud software to close the vulnerabilities, were not implemented by the operators. This allowed attackers to take advantage of known vulnerabilities in obsolete versions of the cloud software to spy out sensitive information stored in the cloud, such as customer data from corporations or personal documents, and then publish them on the Internet or use them for crimes such as extortion. Other vulnerabilities allow attackers to run any program code on the cloud server. This may lead to a complete compromise of the system and its misuse for further criminal activities.

Reaction

The BSI's CERT team regularly informs German network operators about vulnerable cloud systems the BSI is aware of in Germany. Providers are asked to inform their affected customers accordingly and to ask them to close the vulnerabilities.

Recommendation

The BSI advises cloud operators to periodically review the version of the cloud software they use and to install updates made by the manufacturers as soon as possible. The manufacturers of the widely used cloud software ownCloud and Nextcloud provide a free service at https://scan.owncloud.com and https://scan.nextcloud.com with which the operator can check the security status of the cloud based on this software.

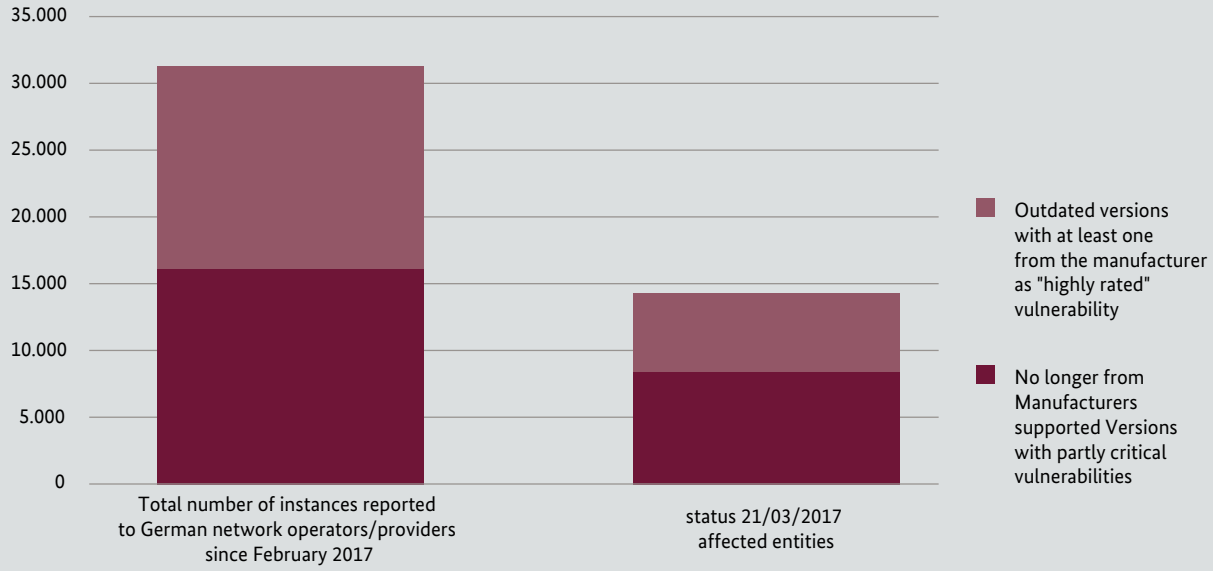


Figure 15 Known vulnerable ownCloud / Nextcloud instances in Germany.

Cooperation with the Federal Office of Economic Affairs and Export Control

The BSI supports the Federal Office for Economic Affairs and Export Control (BAFA) with characteristics or functions of information security in applying for export / shipment authorisations based on the order for the submission of export license applications for goods. The legal basis for this support is the German Foreign Trade Act (AWG), the German Foreign Trade Ordinance (AWV) and the EC Dual-Use Regulation. Its focus is on the field of cryptographic export control and is structured as follows:

I. The support of the German cryptology industry,

II. Protection of approved IT security products and components such as smartcards and technology before re-engineering, manipulation, etc.

The processing of these applications is a cross-cutting task which requires close cooperation with external authorities, the applicants and manufacturers, as well as with the competent divisions / sections. In order to reduce the number of BSI-relevant applications, BAFA agreed to concentrate the processing of applications for export / shipment authorisations on authorised IT security products (see figure 16). This has been implemented since May 2016.

- Participation in the revision of the EC Dual-Use Regulation
- Assessment of pre-requests for information requiring protection, for example, test reports from the CC environment and technology
- Participation in the sale and acquisition of companies in the field of information security in the context of the processing of the decree
- Processing of export requests related to the Chiasmus encryption software, as well as support for the BSI distribution in the application for the export of Chiasmus
- Support of BAFA in providing information on the list of goods (AzG) to determine the export obligation of a product
- Securing of completed MoAs for the export of approved IT security products (from classification VS-CONFIDENTIAL).

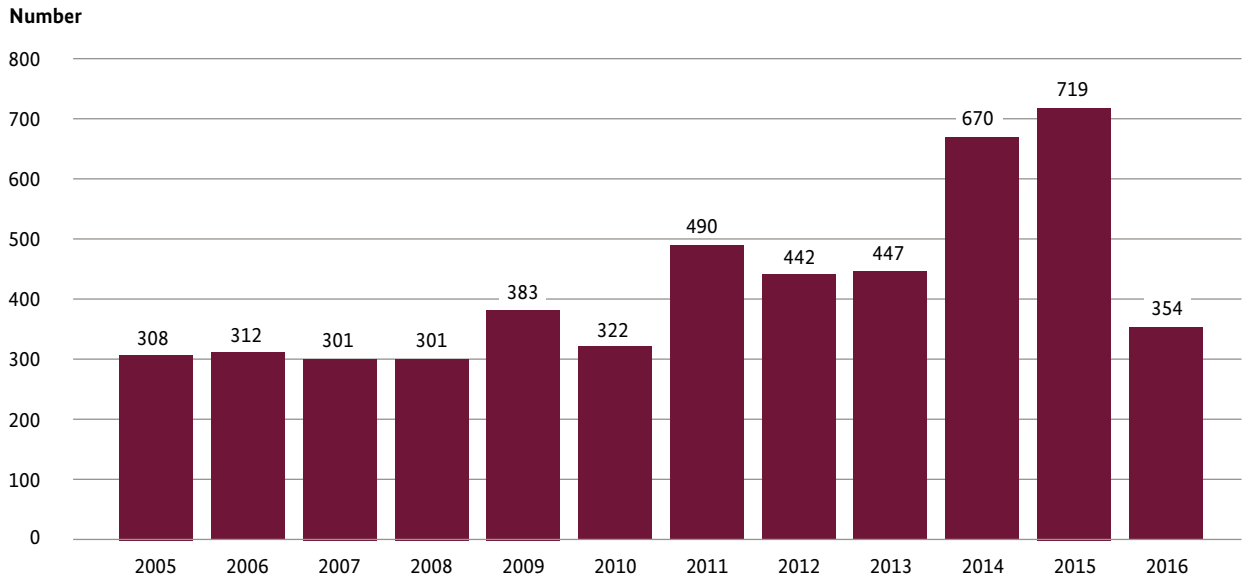


Figure 16 Representation of the number of BAFA applications processed in the BSI from 2005 to 2016.

2.3 Target Audience Business

2.3.1 CERT-Bund and National IT Situation Centre

When dealing with IT security incidents, it is important to react quickly and appropriately in order to prevent the outflow of data, a threat to a third party or the further spread of an attacker in the rest of a network. Computer Emergency Response Teams (CERTs), also referred to as Computer Security Incident Response Teams (CSIRTs), are used to help those affected and their IT security officers and administrators. The emergency response teams have been in existence at the BSI since 1994 and as an independent section since 2001. In 2016, the "CERT-Bund" unit celebrated its 15th anniversary.

In addition to findings from its own analyses, CERT-Bund in its role as a national CERT, receives information on security incidents related to IT systems in Germany from partners and other trustworthy external sources. This includes, among other things, information about malicious program infections, insufficiently secure server services as well as compromised systems or access data. On a daily basis, millions of such events are evaluated automatically and assigned to the relevant network operators on the basis of the IP addresses of affected systems. The network operators are then informed of the abnormalities in their network areas. If the network operator is a provider, the latter is asked to inform its affected customers accordingly.

The national IT Situation Centre of the BSI carries out continuous IT security monitoring. A large number of public and non-public sources are therefore analysed daily, from specialist media to analyst blogs to information from IT manufacturers. This ensures the timely response to newly discovered vulnerabilities or IT security incidents became known. These findings are supplemented by the evaluation of information of different sensors, among others, in the government networks, as well as further analyses.

The BSI's central reporting centre is also located in the IT Situation Centre. Here, incident reports arrive from, among others, Federal Authorities within the scope of the reporting obligations from the Federal Government's Implementation Plan (UP Bund) as well as by the operators of critical infrastructures under the IT Security Act. There are also voluntary notifications, for example, from the Allianz für Cyber-Sicherheit and the UP KRITIS. All these incident reports are recorded in the reporting centre and the further procedure coordinated. Through the overall viewpoint of the centre on all incident reports, it is possible to have a look at the analysis as well as the support of the affected parties in a larger context and to briefly address attack waves or new attack methods. The BSI also uses that information notify its target audiences particularly in the form of state reports, warnings and recommendations.

2.3.2 Mobile Incident Response Teams (MIRT)

With the Federal Government's 2016 cyber security strategy, the focus of the CERT deployment was placed on local support. The BSI is therefore setting up mobile incident response teams (MIRT) that can work directly on site with the affected parties in cases of IT security incidents. The focus is on the facilities of the Federal Administration and operators of critical infrastructures. In exceptional cases, MIRTs can also take action with other companies. At the same time, the existing structures of the CERT-Bund as well as other relevant BSI sections are being expanded.

The main task of the MIRTs is to restore the functionality of the affected information technology systems in the short term in the case of IT security incidents or cyber attacks. This is done in close coordination with the institution concerned.

Typical elements of a MIRT operation are:

- Initial support by telephone and clarification of the necessary prerequisites for an on-site operation: What immediate measures are possible? What support is required? How can this support be provided as quickly and effectively as possible?
- On-site operation to identify the essential problem: What has specifically happened? How has it attracted attention?
- Define the spread of the problem: How far did an attacker spread through the system? Which systems are affected? How can further spread be prevented?
- Clean up the systems, possibly with a previous forensic backup, for evaluation in the laboratory or for law enforcement authorities: What tools or exploits did the attacker use? How can the detection of affected systems be improved? Is a clean-up possible without a new installation?

- Restart the systems: Which order is useful? Which systems could be affected again? What ad hoc measures can provide temporary protection?

The time frame for a MIRT operation should generally not exceed two weeks. If the BSI's capabilities are not sufficient to master the incident, third parties can also be activated, for example BSI-certified IT security service providers. The Implementation Act for the NIS Directive has created the corresponding legal basis for this by supplementing §5a of the BSI Act.

2.3.3 Seals of Approval

The Federal Government's 2016 cyber security strategy provides a seal of approval for IT security in order to strengthen safe and self-determined action in a digitised environment. It is supplemented by a basic safety certificate in order to promote the willingness of the manufacturers of IT consumer products to test and strengthen the IT security in this product area on a sustained basis. International recognition in the European environment will also be taken into account.

The BSI is currently developing the necessary prerequisites to award a seal of approval in close cooperation with the responsible ministries in the exemplary network router category. Manufacturers and associations as well as stakeholders are involved. The result will then be transferred to other product categories with little effort, creating the basis for a broadly applicable, trustworthy seal of approval for IT security.

2.3.4 Alliance for Cyber Security

With the Alliance for Cyber Security founded in 2012, the BSI offers a platform for the open exchange of cyber security information between authorities, companies and other institutions. The aim of the Alliance for Cyber Security is to increase cyber security in Germany and strengthen the resilience of Germany as an economic location against cyber attacks. Alliance for Cyber Security is pursuing a collaborative approach to disseminate up-to-date information on cyber threats, discuss upcoming challenges and work on good practices to securely deal with them.

The expertise gained through collaboration with others is intended to help the participating organisations to improve their cyber security level sustainably and to minimize the risk of becoming victims of a cyber attack. The BSI operates the website www.allianz-fuer-cybersicherheit.de as an information plattform. The digital content is supplemented by open and closed events, such as cyber security days, experience and expert circles. As part of the Alliance for Cyber Security, the partners – usually companies with particular expertise in cyber security issues – provide free content in the form of white papers or seminars.

With the Alliance for Cyber Security, the BSI takes account of an increasingly connected environment. In the face of the increasing threat of cyber attacks and ever new methods of perpetrators, it is necessary to drive the exchange through preventive and reactive measures in cyber incidents in order to benefit from mutual knowledge transfer. This project is of great interest to German organisations: by June 2017, more than 2,270 had registered for participation in the Alliance for Cyber Security – a 30 percent increase year over year. Of these members, more than 100 regularly provide content for the other participants, about 50 distribute the information broadly as partners / multipliers.

Great Reception

Both the commitment of the partners as well as the interest of the participants is remarkable: Last year, the partners of the Alliance for Cyber Security offered an average of one free event per week somewhere in Germany. The BSI can now provide some 130 recommendations on various cyber security topics, which are published on the Alliance for Cyber Security website. Events offered by the BSI are also very popular. More than 200 participants appeared on the 16th cyber security day on 21 February in Hamburg. For the in-house "Training Centre Network Defence," the training was many times overbooked within a few hours of registration opening.

Due to the commitment of the participating institutions, the BSI will further expand the activities of the Alliance in the coming year. Plans are already being drawn up to establish new branch-specific experience circles. In addition, the range of information is being supplemented by additional topics.

UP KRITIS Prevents Malicious Code Propagation

Situation
A company in the petroleum industry observed an attributed malicious code as a mail attachment that the systems used could not recognise. It reported the incident to the BSI on the one hand, following its legal duty according to Section 8b BSIG. On the other hand, it informed the industry contacts, present via UP KRITIS and the industry working group of mineral oil, in an impromptu telephone conference.

Cause and Damage
Sending malicious code is an everyday phenomenon that does not give rise to a warning in the normal case. However, as it became clear in the telephone conference that other companies in the industry had also identified a similar situation, the initial situation changed. As several companies were concerned, there was a reason for a general warning.

Reaction
The BSI sent a corresponding warning to UP KRITIS participants and KRITIS operators registered according to BSIG. Subsequently, the BSI received samples of the malicious code from other warned UP KRITIS participants and was able to analyse them. This led to an update of the warning and to a more appropriate and more targeted recommendation of measures and the necessary awareness.

Recommendation
This reaction shows how, in the case of acute incidents, a long-term established, well-functioning network of trust can be used as in the UP KRITIS in order to exchange findings on an incident and to determine the impact of other KRITIS operators. Without networking and exchange in UP KRITIS, the BSI would not have been able to analyse the situation as quickly as possible in order to be able to issue a precise warning as well as to obtain feedback from the industry.

2.3.5 UP KRITIS and IT Security Act

In 2017, UP KRITIS, the public-private partnership for the protection of critical infrastructures (KRITIS) in Germany, is celebrating its tenth anniversary. Starting in 2007 with about 30 organisations, the number of participants in UP KRITIS has now grown to almost 500 organisations. The participants (KRITIS operators, associations and authorities) work together to keep the supply of business, state and society with important goods and services trouble-free also in the IT age.

The cooperative approach of the Federal Government and business in the protection of critical infrastructures is also pursued with the law for the enhancement of the security of information technology systems (IT Security Act, IT-SiG). The implementation of the legal requirements as well as the identification of who new regulations of the law applies to is actively supported by the KRITIS operators at UP KRITIS.

At the beginning of May 2016, the first part of the Regulation on the Determination of Critical Infrastructures came into force according to the BSI Act (BSI KRITIS ordinance – BSI KritisV). It regulates in the sectors of energy, water, food, information technology and telecommunications which systems are critical infrastructures within the meaning of the IT-SiG, whose operators then have to implement the requirements of the BSI Act. On the one hand, this includes the duty to designate a contact point for the BSI, which must notify significant IT disruptions to the BSI and where in return the operators receive information from the BSI such as situation pictures or cyber security warnings (section 8b BSIG). On the other hand, operators must protect their information technology systems, processes and components, which are decisive for the functionality of the critical infrastructures they operate, from interference (section 8a BSIG).

Implementation of these requirements shall be subject to appropriate deadlines which have begun with the entry into force of the regulation. For the designation of a contact point this means six months, which expired in November 2016 for the operators concerned. This deadline was complied with by the majority of the expected operators, so that for the first part of the regulation, 205 operators registered about 500 installations with the BSI.

Second Part of the Regulation Adopted

The second part of the regulation, which regulates the remaining sectors of health, finance and insurance, transport and traffic, entered into force on 30 June 2017. The BSI calculates a further 800 to 1,000 installations to be registered by the expiry of the deadline six months later. On the part of the BSI, the necessary processes for receiving registrations and incidental notifications have been established and first reports have already been received. Operators are already benefiting from the regulations of the IT Security Act, for example through cyber security warnings or current situation information that the BSI Situation Centre sends several times a week.

To implement section 8a BSIG, sector-specific safety standards (B3S) are developed in various industry working groups of UP KRITIS. The BSI accompanies the creation of the standards and has published several orientation aids as benchmarks. These were also developed in cooperation with the operators of critical infrastructures at UP KRITIS. Upon request, the BSI can determine the suitability of sector-specific safety standards. The first industry-specific safety standard that meets the requirements of the BSI is the B3S water / waste water.

2.3.6 Other Measures for the Business World

Modernisation of IT-Grundschutz

IT-Grundschutz is the most widely used standard for information security in Germany. The modernisation of the tried and tested BSI methodology for the establishment of a solid information security management according to IT-Grundschutz is on the straight line. The goal of the modernisation is to enable particularly small and medium-sized enterprises to simply enter into their own security management. Basic projects could successfully be launched: At CeBIT 2017, the new standard 200-2 for IT-Grundschutz methodology was presented as a community draft and at the Hanover Trade Fair Industry 2017 the BSI standard 200-1 to the foundation of the information security management. The standard 200-3 on the topic of risk management has already been presented in October 2016 as part of the IT security trade fair it-sa. The three standards replace their predecessors 100-1 to 100-3.

At this year's trade fair it-sa in October 2017, the modernised IT-Grundschutz will be published in finalised version. It comprises the BSI standards 200-1,2,3 as well as the new IT-Grundschutz compendium with around 80 essential modules on various aspects of information security. After the extensive revision, the IT-Grundschutz is now more lean, practical and flexible useable. This applies in particular to the new building blocks in the IT-Grundschutz, which now contain all essential information in around ten pages. This saves users time and resources.

Cloud Computing Compliance Controls Catalogue (C5)

In February 2016, the BSI introduced the Cloud Computing Compliance Catalogue (C5). It consists of three essential parts that address requirements for security, transparency and audit of cloud services. The 114 security requirements, which are divided into 17 thematic sections, represent the minimum requirements that professional cloud services must meet for business-relevant data and processes. For the most part, they come from other standards such as the ISO / IEC 27001 or the Cloud Controls Matrix of the Cloud Security Alliance, since a high level of informal consensus has now been reached within the cloud security community.

Some areas are more emphasized by the C5, such as emergency management and cryptography. In the transparency requirements, the C5 helps determine whether the framework conditions of the cloud service meet the requirements of the cloud customers. Proof of compliance with the requirements of C5 is provided by auditors. Based on the international standards ISAE 3000, ISAE 3402 and SOC 2, the C5 makes some concretisations. The goal is to make the review and report meaningful so that the cloud customer has a valid content for his own risk management.

Through the use of proven standards, newly combined and supplemented by the expertise of the BSI, the C5 created a standard that immediately received international attention. Up to the time of the publication of this report, three cloud providers have already been audited: Amazon Web Services, Fabasoft and Box; more are expected.

Figure 17 Arne Schönbohm at „BSI in Dialogue with Politics“

European Secure Cloud (ESCloud)

The European Secure Cloud (ESCloud) is an initiative of the BSI and the French partner organisation Agence nationale de la sécurité des systèmes d'information (ANSSI). Both authorities have defined common criteria for cloud security. Cloud providers who demonstrate these criteria through a C5 audit or a certification from ANSSI (SecNumCloud) and provide their services in Europe are given the ESCloud label as a quality feature. The first labels are to be awarded in 2017, when the associated process is established. In addition, other European countries should be motivated for further cooperation.

For cloud users, the cloud label makes it easier to select an appropriate cloud provider. Through the use of the label, vendors can make clear that their cloud services meet the basic security requirements, either defined by the German C5 catalogue or the French SecNumCloud.

2.4 Target Audience Society

2.4.1 Protection against the Influence of the Bundestag Election

On 24 September 2017, the election to the 19th German Bundestag takes place. Although the citizens vote in election offices with pen and paper, digitalisation also plays a key role at the Bundestag election. Electronic communication and information processing is used, among other things, in the organisation of the election and in the determination of the preliminary election results. In addition, the previous election campaign also takes place over digital media, such as on social networks, blogs and other web offers. Twitter and Facebook are now important sources for informing citizens about candidates and parties.

Against the backdrop of the US and French reports of cyber attacks related to the presidential elections held there (see info box electoral influence Electoral influence – security incidents in the context of political elections page 65), there is also concern in Germany that perpetrators could try to influence the Bundestag election 2017 on the digital way.

Although the BSI does not have any concrete information about planned cyber attacks on the Bundestag election, Germany has to be prepared for this scenario. Possible targets for cyber attacks in the context of elections are, in particular, bodies such as parliaments, parliamentarians and authorities, parties (party headquarters, offices, candidates), media (journalists, editors, publishers, online platforms such as Facebook and Twitter) and IT used for the Bundestag election at all Federal Levels.

Within the scope of its legal mandate, the BSI provides extensive information and service offers to protect the 2017 Bundestag election. First, there is the consultation and support for the Federal Election Commissioner, who is responsible for the preparation and implementation of the Bundestag election at the Federal Government

Election Influence – Security Incidents in the Context of Political Elections

Situation
In the recent past, a number of targeted cyber attacks have been reported in the political environment, especially regarding elections. In the run-up to the US presidential elections, for example, computers of the Democratic National Committee (DNC) were compromised. The attackers captured a variety of documents. US intelligence agencies concluded in an investigation report that these attacks were controlled by two Russian hacking groups who were active in parallel in the Democrats' network.

Media also reported in June 2017 about the release of an alleged top-secret report of the NSA on spear phishing attacks on US electoral authorities as well as on US service providers operating in this area.

In March 2017, several thousand Twitter accounts were compromised on the day of parliamentary elections in the Netherlands. The attackers published messages on the affected Twitter accounts advertising for the referendum that Turkish leader Erdoğan was striving for, at the same time fighting against Germany and the Netherlands. In addition, a large number of defacement attacks were recorded in which, for example, contents of websites of established institutions were manipulated and abused for propagandistic purposes.

In the context of the French presidential elections in May 2017, the party "La République en Marche" with its presidential candidate, Emmanuel Macron, was affected by cyber attacks. The perpetrators captured and published internal documents.

Cause and Damage
With the help of fraudulent and phishing e-mails, hackers have infected selected recipients with malicious software in order to steal the passwords of those affected. In this way, they have acquired a large number of documents and extensive e-mail correspondence. This has led to some compromising publications. The abuse of the Twitter accounts in the Netherlands took place via the web application or "app" twittercounter.com, with which users can manage their Twitter accounts and generate user statistics and reports. Twitter users must explicitly allow apps like twittercounter.com to access their own Twitter account so that the app can post tweets via their account. By compromising the app twittercounter.com, attackers were able to publish content on Twitter accounts.

Reaction
The Bundestag election in 2017 is the focus of the BSI's continuous situation monitoring, also in exchange with other European countries such as France and the Netherlands, where elections took place. The BSI supports the Federal Election Commissioner and advises him, for instance on selecting and implementing security measures, in particular for the strengthening of IT systems and networks.

As part of its advisory activities on IT security issues, the BSI has also informed parties and party-affiliated foundations about the possibility of cyber attacks and conducted penetration tests on request at particularly critical points. In addition, the BSI has recommended measures for digital personality protection. Digital personality protection is the protection of the activities of important personalities in the digital space. In addition to the protection of private e-mail mailboxes, this also includes measures such as the verification of Twitter and Facebook accounts, in which the BSI has supported numerous representatives and candidates at their request.

Recommendation
On the one hand, there is a need to critically question reports and announcements on the Internet, especially in social networks. On the other hand, parties, politicians and institutions in the political environment increasingly have to adapt to targeted cyber attacks and implement appropriate security measures at an early stage. Twitter users should, for example, regularly check which apps have access to the respective Twitter account.

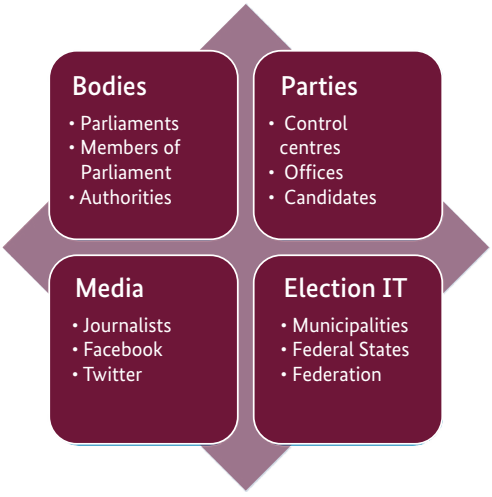


Figure 18 Possible targets of cyber attacks

level (see https://www.bundeswahlleiter.de). The BSI advises him on organisational and technical issues of information security and provides recommendations on the conception and implementation of security measures. On request, the BSI has carried out penetration tests at particularly critical points. In addition, the BSI has prepared an information package with instructions and recommendations for the regional election coordinators in coordination with the Federal Election Commissioner.

Information security, however, cannot be achieved by measures of operators and administrators alone, but also requires always the involvement of users. For example, this concerns the safe handling of social networks, mobile IT systems and e-mail. Within the framework of several information events, the BSI has therefore also raised awareness of cyber security risks with Members of Bundestag in the context of elections in the Federal Government and the Federal States, and has drawn attention to relevant offers with indications and recommendations. This includes two events of the series "BSI in Dialogue" with members of the Federal Parliament and members of the state parliament in Düsseldorf and Berlin.

The BSI has also offered political parties specific information, counselling and support services tailored to the subject of elections. This has met with great response. In addition to the protection of information and communication systems, the risk of discrediting people through the misuse of digital identities has also been regularly addressed. The BSI therefore offered the members of the Bundestag and the candidates a "digital personality protection." Overall, there is a need to critically question reports and messages on the Internet, especially in social networks. Parties, politicians and institutions in the political environment must increasingly deal with the fact of targeted cyber attacks.

As a platform for the handling of incidents and for dialogue with media on the subject of information security, the BSI primarily uses the cooperation in the UP KRITIS, and there in particular the working group "Media." In this way, the BSI also discussed the special security aspects of the Bundestag election with the media companies. The BSI is also in direct contact with social media providers on security issues.

In addition to the consulting and support service offers, the Bundestag election is now also a focus of situation monitoring at the National IT Situation Centre. This ensures that relevant events related to the Bundestag election can be responded to immediately, such as by warning or appropriate protection measures.

2.4.2 Digitalisation Projects in Germany

Increasing digitalisation and networking in society increases efficiency, optimises processes and leads to more comfort by linking product components and systems to one another in a communicative manner. On the other hand, the threat potential increases significantly as the number of attack points increases, communication infrastructures become more complex and the amounts of data to be processed are multiplied. The probability of successful attacks on digitised infrastructures is therefore increasing.

Successful digital transformation can only be achieved if general-purpose security standards are developed and deployed at an early stage and measures implemented to ensure the trustworthiness of digital infrastructures ("Privacy & Security by Design"). This is why national reference markets with secure product components, systems and communication infrastructures are essential to take a leading design role in future digital markets and to shape the international standardisation on this basis.

Healthcare

Also in the field of healthcare, digitalisation (eHealth) is both a pronounced factor and an opportunity. The example of the telematics infrastructure shows that the increasing networking of healthcare providers raises the efficiency of the care system and at the same time enhances the safety of patients. New applications, such as emergency data management or the eMedication plan will make a further valuable contribution to this.

The use of certified components in security-critical areas of this infrastructure supports the goal of the further digital development of secure, sustainable and comprehensive medical care in Germany, while also considering data protection issues.

But also with the individual equipment of patients with electronic devices (health card), digitalisation opens up new hitherto unachieved possibilities to compensate any existing medical-related personal deficits and thus increase the quality of life of those affected. However, electronic access to the devices – e.g. for individual adaptation / adjustment or for (remote) maintenance – always creates a certain risk of unintended data leaks or manipulation. Once again, the BSI's objectives and demands for data security are of vital importance.

Secure Identification of Natural and Legal Persons and Things

For the implementation of digitalisation, the secure identification of people and things is of crucial importance. This is the only way to ensure trust in electronic services and processes. The development of secure eID technologies and their standardisation is therefore one of the core competencies of the BSI.

With regard to the digitalisation within the European Single Market, the "eIDAS Regulation" (EU) 910 / 2014 established the first uniform Europe-wide valid framework for the mutual recognition of electronic identification methods and trust services on a European level. With its expertise, the BSI participates in its further development and technical implementation in all areas.

In February 2017, Germany launched the notification of the online identification function of the ID card and the electronic residence permit at the highest level of assurance in accordance with the eIDAS Regulation. Upon completion of the notification, all EU Member States will be required to open their electronic administrative procedures for the online identification function from September 2018 onwards. Companies in other EU countries can also recognise electronic identity verification on a voluntary basis. The BSI has performed the technical preparatory work for the notification of the online identification function and accompanies the entire notification process from a technical point of view.

In addition, the mobile use of eID technologies such as the development and certification of the mobile IDApp2 for ID cards and smartphones as a card reader also plays a significant role. The BSI is involved in corresponding standardisation committees such as the NFC Forum and FIDO.

Identification Procedures (TR 03147)

In practice, however, very different procedures with different security properties have been established for identification. The BSI is therefore developing, in coordination with stakeholders, criteria for assessing the level of assurance of procedures for the identity verification of natural persons and publishing these in Technical Guidelines (see BSI TR-03147). In this way, a uniform security assessment of identification methods, such as processes with personal presence or video-based procedures, will be able to be facilitated in the future.

Smart Borders

A completely different field of application of innovative technologies can be found in the classical border control process. While travellers from European countries have been able to carry out the self-service border control for several years at the Schengen external borders with the German Federal Police's EasyPASS system, the digitised border control system is being further enhanced with the introduction of the European Entry- / Exit System (EES). The system then allows the biometric enrolment and search of third-country nationals and documents the individual arrivals and departures into the Schengen area. The BSI supports the Federal Police in the areas of secure inspection of official travel documents (optically and electronically) and in the biometric data collection of travellers. This creates an overarching tool for identity management in the common area of freedom of movement. The requirements and certifications of the BSI will ensure a consistently high level of process security.

Implementation of Energy Transition

On behalf of the Federal Ministry for Economic Affairs and Energy (BMWi), the BSI develops protective profiles and technical guidelines as well as test methods for the smart meter gateway as a central communication platform for intelligent measuring systems. Together with the technical standards of the BSI, the law for the digitalisation of the energy transition creates a binding framework for the safe and privacy-compliant use of charging stations and already shows how the minimum requirements must be designed to safely integrate the charging station infrastructure of electric cars into the smart power grid. In this area, Germany is a pioneer in Europe.

Smart Home / Internet of Things (IoT)

Smart Services, Smart Home, Smart Building and Smart City (Urbanisation 2.0) are examples of how advancing digitalisation is entering almost all areas of life through the Internet of Things. In addition to the associated improvements in comfort, however, a gateway for cyber attacks arises at the same time. Especially in the consumer market segment, many devices are insufficiently or not at all protected from cyber attacks. In addition to personal threat to the user (such as accessing or spying on property), the sheer volume of IoT devices can also be abused for DDoS attacks and cause enormous damage to third parties.

The guarantee of "security by design" for IoT devices is an important goal of the BSI. It can be achieved by creating compact and modular safety standards and anchoring them internationally. In this context, functionalities for secure software updating over the complete life cycle of the devices, strong and updatable cryptographic mechanisms and the use of embedded hardware security components play important roles for the execution of safety-critical functions.

Connected Driving and Intelligent Traffic Systems

Digitalisation also has an impact on road traffic. Intelligent transport systems in which connected vehicles and infrastructure components exchange data should prevent accidents and traffic disruptions in the future and make driving more comfortable. However, such systems are only trustworthy if, for example, the authenticity of the messages exchanged is guaranteed. In this context, the BSI is involved in security guidelines for the necessary public-key infrastructures in vehicle-to-vehicle and vehicle-to-infrastructure communication.

Numerous car models already offer comfort functions based on a mobile connection to the Internet. Here as well, there is the danger of cyber attacks, as has been demonstrated in the past few years for individual vehicle models. Together with the Federal Ministry of Transport and Digital Infrastructure (BMVI) and other authorities, the BSI is discussing what minimum requirements have to be fulfilled for IT security in connected and automated vehicles in the future.

2.4.3 Platform for Discourse on Secure Information Society

The BSI has continued its course of promoting overall social discourse on cyber security issues, already intensified in 2016. Within the framework of the project "Digital Society: Smart & Secure" (https://www.bsi.bund.de/susi), the activities were bundled and the open exchange of interests was driven in dialogue with representatives from civil society, culture, science, business, industry and administration.

With its "Secure Information Society Ideas Workshop," the BSI offers a platform to discuss issues of cyber security in a digitised society with a broad spectrum of actors. The focus of the events in February and June 2017 was on multifaceted and constructive debates. While the central questions at the event in February 2017 around the issues of "security and technology," "responsibility" and "trust" were identified with the help of small group discussions in the form of a "world café," the reflection of the results of the empirical analysis and the joint development of a discussion paper were in the foreground in June 2017. On the basis of expert interviews, a representative population survey and a survey of 20 citizens in an online community, joint impulses were developed for a secure information society.

The results of the process and the discussion paper will be presented to the public in September 2017 in Berlin. They provide the basis for the BSI's ongoing work in this area. The fruitful discourse has motivated the BSI to consistently pursue this path in order to continue to shape a secure information society in the context of overall social exchange.

2.4.4 Other Measures for Society

Citizen Services of the BSI

An important task of the BSI is informing citizens and raising awareness for the safe handling of information technology, mobile communications and the Internet. At https://www.bsi-fuer-buerger.de a specially designed Internet site is provided for private users. It deals with the diverse topics and information on the subject of IT and Internet security in such a way that it is also comprehensible for technical laymen. Besides pure information, the BSI offers concrete and actionable recommendations for citizens, such as e-mail encryption, smartphone security, online banking, cloud computing and social networks. The website received an average of 243,000 visitors a month during the reporting period. This represents an increase of 40 percent from the previous year.

On social media, the BSI offers Internet users the opportunity to learn about IT security through its Facebook page (www.facebook.com/bsi.fuer.buerger) and Twitter channel (www.twitter.com/BSI_Presse), active since March 2016, and to enter into dialogue with the BSI. As of 30 June 2017, it had 31,738 fans (Facebook) and 7,483 followers (Twitter). Both communication channels are primarily used to quickly and extensively provide information on IT security incidents. Resonances show that the BSI is highly valued as an expert IT security information centre.

Private users can also contact the BSI by telephone at 0800-2741000 or by e-mail at mail@bsi-fuer.buerger.de with questions about IT and Internet security. The service centre of the BSI receives an average of around 450 inquiries from private users each month.

In addition, the BSI provides a free warning and information service with its "Bürger-CERT," which provides citizens and small companies with fast and competent information about vulnerabilities and other risks, providing specific support. Currently, around 105,000 subscribers use this information service, about 3,000 more than in the previous year. The biweekly Bürger-CERT newsletter "Secure • Informed" provides an overview of the most important IT security news. In 2017, the entire Bürger-CERT offer was integrated on the website "BSI für Bürger." Since then, visitors to the online portal can find all important information from warnings to basic IT knowledge bundled in one place.

European Cyber Security Month (ECSM)

In October 2016, the European Cyber Security Month (ECSM) took place throughout Europe under the leadership of the European Network and Information Security Agency (ENISA). The public was informed and made aware of diverse topics in cyber security. The BSI assumed the role of the national coordination centre in Germany and also took part with its own events. 73 partners were inspired to participate in over 120 events at the ECSM. The events ranged from employee awareness in companies and live hacking campaigns to webinars and information events. An overview of these events can be found at www.bsi.bund.de/ecsm.

The BSI itself presented on the main topics "Safe online payment," "Recognise cyber dangers," "Fit in IT security" and "Smartphone & Co - secure mobile." For this purpose, it created, among other things, a series of animated explanatory videos. On Facebook, a cyber-security ABC was posted throughout October, where different terms were explained. The BSI's events were rounded off with an online quiz at www.bsi-fuer-buerger.de.

In the run-up to the ECSM, experts in security consultancy at the BSI addressed questions from parents and (media) educators on the topic of basic protection in a webinar with klicksafe.de in late September 2016. Together with the Police Crime Prevention of the Federal States and the Federal Government the BSI also interviewed citizens online, asking what protective measures they use, where they inform themselves about IT security and what experiences they have had with cybercrime. More than 1,600 citizens responded to the survey.

The BSI also invited representatives from civil society, media, administration and think tanks to the ECSM at the European House in Berlin on 5 October 2016, discussing, among others, how cyber security can be shaped for society. Participants discussed, among other things, aspects of measuring the success of awareness-raising measures, the integration of IT security measures in products for private users and education in schools and educational institutions.

Cooperation with Verbraucherzentrale Nordrhein-Westfalen

An important part of the BSI's cooperative design approach is its trustworthy cooperation with recognised players in the area of cyber security for society. The BSI has already worked successfully and constructively with the Verbraucherzentrale NRW (consumer advice centre North Rhine-Westphalia) in several fields. This partnership was now strengthened with the signing of a Memorandum of Understanding in early March 2017.

By combining the BSI's technical expertise on the one hand and the Verbraucherzentrale NRW's consumer perspective and legal competences on the other, the joint work is able to increase information security for citizens. An example of this successful cooperation is the current legal action against a smartphone vendor selling products with vulnerabilities that are no longer fixable. This action was only possible on the basis of the BSI's technical examination.

Cooperation with the Police Crime Prevention of the Federal States and the Federal Government

Heightening risk awareness, enabling self-protection and preventing private users from being victims of cybercrime or even being unwittingly abused: these premises are part of the BSI's prevention work in the The Police Crime Prevention of the Federal States and the Federal Government (ProPK). In early April 2017, BSI President Arne Schönbohm and Gerhard Klotter, Chairman of project leadership of ProPK in Stuttgart, signed a joint agreement on the strategic cooperation between the two organisations.

The BSI and ProPK have already been working together in the past on topics related to IT and Internet security. With the online application "Safety Compass," they explain ten common security risks on the Internet, and the media pack "Wrong click" for school teaching mediates adolescents on security-conscious behaviour in daily digital life regarding such issues as cyber bullying, social networks and personality rights.

2.5 Cryptography as the Basis for IT Security

2.5.1 Germany as Top Encryption Site

The "digital agenda" adopted by the Federal Government, as well as the "Charter on Strengthening Trustworthy Communication," set the goal of making Germany the "top encryption site in the world" for the protection of citizens, business and administration against spying on and manipulating communication.

The BSI's work is oriented towards this goal. It relies on the use of strong cryptography as the basic prerequisite for ensuring the authenticity, integrity and confidentiality of digital information.

In order to promote this goal, the "Focus Group Encryption" was established as an initiative of business, trade associations, consumer organisations as well as politics and science. In the autumn of 2015, it launched a "Charter for Strengthening Trustworthy Communication" (www.krypto-charta.de), which has already been signed by a large number of companies and associations. The BSI actively supports the work of the focus group, contributed to the formulation of the Charter and was one of the first signatories alongside the BMI.

Signatories to the Charter are committed to, among others,

- Simplicity,
- Technology neutrality / relevance / standards compliance,
- Transparency and trustworthiness
- Security made in Germany / Europe.

The aim is to promote user-friendly, transparent, secure encryption solutions and to guarantee strong algorithms without traps to strengthen citizen and small business in the security and integrity of the digital world.

The main focus of the focus group's activities lies on end-to-end encryption of e-mail communication. This allows users to protect the contents of their e-mails from the sender to the receiver without the intermediary systems being able to read them.

The encryption of e-mails on the transport route, between the servers of the large e-mail providers on the Internet, is already well-established today (transport encryption) and is normally automatically provided without the participation of users.

User-specific end-to-end encryption, however, is still far too rare, especially in e-mail communication, due to lack of awareness and offers, and is still a niche application in contrast to the now established encrypted messengers. User-oriented, technology-neutral and secure offers need to be created and promoted. Among other things, the initiative "People's Encryption" and the solutions offered by 1&1, GMX and Web.de are creating positive development.

The focus group encryption also uses organised speed dating to bring together companies that contribute to encryption solutions. Synergy effects are to be found and used efficiently in order to optimise offers for businesses and citizens. More recently, it has already been noted that there are more and more user-friendly offerings on the market that are designed to promote the use of strong encryption.

The BSI also has several projects around secure e-mail communication (e.g. based on the free Gnu Privacy Guard / GnuPG cryptography system). In addition, service providers wishing to provide De-Mail services must be accredited by the BSI. The BSI's Technical Guidelines also provide guidelines for secure e-mail transport, De-Mail and for the widespread use of strong cryptography in IT security products.

2.5.2 Botan – Secure Implementation of an Universal Crypto Library

Cryptographic libraries are often used as core components in security applications. They are of central importance to achieving security objectives. The choice of available libraries for this application area is large and steadily growing. In the TLS environment, there are currently around 15 open source libraries, such as the well-known and widely used OpenSSL. Due to the typically large scale, high complexity and increasingly expanding structure of these libraries, however, actual usage in crypto products is error-prone and an evaluation of cryptography is practically impossible.

For these reasons, the BSI is conducting the project "Secure implementation of an universal crypto library" with the contractor Rohde & Schwarz Cybersecurity GmbH. The goal is to provide an open source, secure, concise, controllable, well-documented and evaluable crypto library that is suitable for many application scenarios and can also be used in applications with increased security requirements.

To this end, the library Botan was chosen as a suitable basis for further development in an initial analysis phase from all common open source crypto libraries. In the subsequent development phase, Botan was cryptographically examined and existing deficiencies were remedied. Missing crypto primitives and standards have been reimplemented according to the BSI Technical Guidelines, the test routines have been improved and a test specification has been prepared. In addition, resistance to side-channel attacks was improved by suitable software countermeasures and the possibility of incorporating cryptographic special hardware was created. Botan's documentation has been improved and expanded.

All changes and extensions to Botan made during the project were returned to the original project. The library developed by the BSI corresponds essentially to the current, publicly available version of Botan (see https://botan.randombit.net/).

In order to ensure the security and validity of the crypto library in the future and to respond appropriately to new scientific developments, security threats and deployment scenarios, the library will continue to be maintained in the ongoing maintenance phase during the coming years and as far as possible synchronized regularly with the official Botan version.

2.5.3 BSI Project: Evaluation of Lattice-based Crytographic Algorithms

In view of the possible development of a universal quantum computer, today's public key cryptography has to be replaced or supplemented as soon as possible by algorithms which additionally are resistant to attacks using such quantum computers. Hash-based signatures are already well-understood and standardised today. These are considered to be resistant to quantum computers. However, there are no hash-based algorithms for key agreement or encryption. Proposals for such algorithms are based on

Virus Protection

Modern virus protection software is still indispensable for most IT users. Private users should at least use a well-tested, free Internet security suite under Microsoft Windows. Chargeable versions are even safer, offering a larger range of functions and better support without financing themselves with advertising or evaluating user data.

For larger networks, professional IT users should only use proven enterprise products that have a much broader range of functions compared to consumer products (e.g. central management, application control, weak-point scanner). Enterprise protection consists of a variety of different products that combine to form a complex IT security infrastructure. The most important component is endpoint protection, which includes the most detection procedures. Gateway products are essential, similar to spam filters, but do not provide sufficient protection on their own.

The pure recognition performance of established protection programs differs very little. However, the detection rates for different configurations of the same product may be significant. It is therefore important to optimally configure the chosen product, to master it reliably and to adequately react to recognised threats. The use of resources in planning, implementation, operation and auditing is much higher than in the past.

Connecting to the manufacturer's cloud increases the detection rate significantly, but also entails the risk of unwanted data transmissions. The BSI therefore calls on manufacturers to specify to their customers what data is transferred to the cloud and in what manner it is used.

In order to better detect malicious software, different sensors are now connected and partly use central analysis components. Deciding on a main supplier of protective technology can therefore offer advantages. This portfolio can then be supplemented by additional products from other manufacturers. In the case of protection software, which mainly operates with known search patterns (signatures) (e.g. at the gateway or data carrier locks), a multi-vendor or multi-engine strategy is still useful.

Modern protection programs recognise many, but not all, attacks. They offer only limited protection against targeted attacks or new attack techniques. In addition to protection programs, familiar basic security measures should always be implemented: a secure network and system architecture, regular updates and secure authentication with strong passwords and two-factor authentication.

In the enterprise sector, special analysis systems and virtualisation techniques are increasingly being used. In this process, suspicious files are automatically executed and analysed in a secure environment, while applications are encapsulated so that a malicious program cannot access important data and programs.

- the difficulty of efficiently decoding general error-correcting codes ("code-based cryptography"),
- the difficulty of calculating isogenies between elliptic curves ("isogeny-based cryptography") or
- the difficulty of certain problems in mathematical lattices ("lattice-based cryptography").

On behalf of the BSI, researchers from the Technical University of Darmstadt produced a study on the "evaluation of lattice-based cryptographic algorithms." The aim of this study was to obtain an analysis of the previous publications on lattice-based cryptography (key agreement, signature and encryption). For this purpose, the theoretical fundamentals were collected in a first part, that is, the various lattice problems and reductions between them, as well as the various approaches to solving lattice problems (for example reduction of a lattice basis). This forms the basis for evaluating the security of lattice-based algorithms. The second part of the study consists of an overview of these algorithms and an evaluation of selected algorithms based on the results of the first part. The study is published on the BSI website.

2.5.4 Study "Analysis of Randomisation in Virtualised Environments"

A study by the BSI investigated, how virtualisation techniques, such as those used in cloud services, can affect the entropy of operating system noise sources, and what can be done to ensure the supply of the virtual machines (VM) with enough randomness. The open source random number generator of Linux was investigated as an example in virtual machines that run on different virtual machine monitors (VMM) such as KVM, Oracle VirtualBox, Microsoft Hyper-V and VMware ESXi.

As a result, adequate entropy supply of the Linux VMs was possible in all combinations with a corresponding configuration. Different sources of noise, however, fulfilled their tasks differently. Depending on the application scenario, problems could arise shortly after the system start, for example, for the quality of the random numbers. Using a questionnaire, users are able to analyse these, if they come across such such problems, so that they can request the critical information from their system suppliers beforehand.

In principle, users must trust their VMM (and its operator) and should not rely on a sole source of noise.

- Software-based noise sources that require hardware support for their entropy recovery may be most likely to be problematic, and therefore need to be most closely examined for their suitability for the application environment.
- Software-based noise sources that evaluate high-resolution time stamps for system events work just as well and sometimes even better in virtual environments than in non-virtualised environments.
- Hardware noise sources are mostly unaffected by virtualisation. In a suitable combination, the VMM can also support its guest system in the extraction of entropy.

2.5.5 Technical Guidelines BSI-TR-02102 and ECC side-channel guideline

BSI-TR-02102

An important task of the BSI is to provide recommendations to the Federal Administration, companies and private users for the secure use of IT systems, for instance in the form of Technical Guidelines (TR). They pursue the objective to spread appropriate IT security recommendations and address all parties involved in the installation or safeguarding of IT-systems. They complement the technical test specifications of the BSI and provide criteria and practices for conformity evaluations ensuring the interoperability of IT security components as well as the implementation of defined IT security requirements. The recommendations help companies, for example, to operate web servers securely, or authorities of the Federal Administration to implement a data exchange procedure in such a way that the data can be transferred securely according to the current state of cryptographic technology.

For this purpose, the BSI has been producing and maintaining, among others, the BSI-TR-02102 Technical Guidelines for many years. The series is currently comprised of four documents that contain general cryptographic recommendations on key lengths and cryptographic algorithms (Part 1) as well as specific recommendations for the use of the cryptographic protocols TLS, IKE / IPsec and SSH (parts 2 to 4).

The Technical Guideline BSI-TR-02102-2 (TLS) provides the basis for the TLS minimum standard which makes this technical guideline binding for the Federal Administration. All Technical Guidelines are updated regularly once a year and, if necessary, additionally to react to new developments.

Since November 2016, all four Technical Guidelines are also available in English on the BSI website. One of the most important changes in the 2017 versions is the announcement that the BSI will increase the security level from 100 to 120 bits as of 2023.

ECC Side-channel Guideline

Within the framework of the Common Criteria (CC) certification, the BSI supports manufacturers, evaluators and certifiers by issuing application notes and interpretations in the schema (so called AIS). AIS46 “Information on the evaluation of cryptographic algorithms and additional notes for the evaluation of random number generators” includes, among others, a guideline with minimum requirements for the side-channel analysis of implementations of elliptic curve cryptography (ECC). It provides notes on the side-channel-resistant representation of curves, curve points and the implementation of arithmetic. In addition, side-channel-resistant aspects of common protocols such as ECDH, ECDSA, ECIES and PACE are discussed.

This guideline, originally from the year 2011, was updated in 2016 in cooperation with the scientific community, manufacturers, CC testing laboratories and CC certifiying authorities, considering newer attack methods. It will continue to be updated over the coming years.

3 Overall Assessment and Summary

3 Overall Assessment and Summary

Gateways for Cyberattacks

During the reporting period from July 2016 to June 2017, the risk situation is continuously tense and at a high level. The main gateways for cyberattacks are unchanged and remain critical:

- Vulnerabilities exist in software, and in some cases even hardware products, which are used most often. These vulnerabilities enable attackers to recover information or gain control over systems (Chapter 1.4.1).
- Detected Vulnerabilities are reported too slowly and incompletely, manufacturers make updates available too late and users implement recommendations and updates not directly and only incompletely (Chapter 1.4.1).
- Botnets that are structured and operated in an organised manner still pose a significant threat to IT security (Chapter 1.4.4). They are used to widely spread malware or spam mail or to sabotage the availability of services. Lately, botnets from IoT devices such as the Mirai botnet have become a major threat.
- The sudden rise in cases of ransomware shows that cyber criminals have found a new way of extorting particularly large amounts of money (Chapter 1.4.3). Anonymous payment methods, such as bitcoin, facilitate this approach. By blocking the data and the digital identity of the victim until payment or deleting without payment, a form of "digital hostage-taking" has developed.
- The "human factor" always plays a crucial role when attacks are carried out through social engineering (Chapter 1.4.6). Calculated phishing attacks that are addressed to individual companies or employees have occurred more often in the past few years. Assailants put particular effort into CEO frauds. These are variants of social engineering that cause high damage sums (Chapter 1.4.7).

The Challenge of Digitalisation

At the same time, it is becoming clear that in the period under review the digitalisation of all areas of life along with rapid technological development presents great challenges to government, the business world and society. Increasing digitalisation and networking lead on the one hand to efficiency gains through simplified processes, to greater transparency through improved communication possibilities and to more comfort in everyday life, since components and systems are linked to one another in a communicative manner. On the other hand, the threat potential increases significantly as the number of attack points increases, communication infrastructures become more complex and the amounts of data being processed are multiplied. The probability of successful attacks on digitalised infrastructures is also therefore increasing. Almost daily, there are new attack points and far-reaching possibilities for cyber attackers to spy out information and know-how, sabotage business and administrative processes or to criminally enrich themselves at the expense of third parties:

- The Internet of Things is increasingly becoming a new source of risk for IT security. The fact that IoT devices can be easily attacked and that their security does not play an adequate role in production or the customer's purchasing decision contributes significantly to this (Chapter 1.3).
- Failures or disorders of industrial control systems – particularly in the area of critical infrastructures – usually have serious physical effects, as power cuts or disorders of logistics or production processes for example. Changes of used technologies and infrastructures increase in the course of Industrie 4.0 (Chapter 1.4.11).
- The influence on political processes through cyberattacks is a relatively new phenomenon, usually by professional and presumably state-controlled attack groups. Attackers target private e-mail accounts, for example, and attempt to gain information that they publish later – during political campaigns, for example – to gain influence on the reputation of candidates or the voters' formation of opinions. This has led to the emergence of various incidents at home and abroad that have indicated that, not only democratic institutions, but also democratic procedures such as elections are increasingly becoming the focus of cyber attackers.

IT and Cyber Security as Prerequisites

Information security in government institutions and authorities, in companies and organisations, but also for private users, has to be continually adapted at high speed to the dynamic conditions that all-encompassing digitalisation brings.

In order to not fall behind in the fight against cyber attackers, the security of the systems used in government administration, in business and by the end user must be ensured from the beginning, without significantly limiting the possibilities of digitalisation. To enable the implementation of the paradigms "security by design" and "security by default," IT and cyber security need to be a matter for management. Only if an appropriate level of security is ensured from the beginning can digitalisation projects lead to success that everyone benefits from. After all, cyber security is not a brake on innovation, but its guarantee.

Defence and Prevention from a Single Source

The BSI, as the national cyber security authority, shapes information security in digitalisation through prevention, detection and reaction for government, business and society, with a strong cooperative approach and numerous partners. As an independent competence centre for IT security in Germany, as a multiplier and a central coordinating body, it ensures holistic and consistent implementation of its various tasks, for example, of cyber security strategy, the IT Security Act and the NIS Guidelines Implementation Act. The BSI's perception of its various and different tasks benefits from close cooperation with experts from various special fields of IT security. This allowed the BSI to react quickly and with extensive expertise to serious IT security incidents such as WannaCry or Petya. This ensures that knowledge from operative cyber defence or from permanent hardware and software analyses as well as from basic cryptography work can be used for standardisation and certification without any delay. With this strategy, the BSI designs IT security from a single source.

This also applies to the cooperation between the government and enterprises in the design of more cyber security, especially in the KRITIS area. The IT Security Act has created a legally binding framework that must be consistently implemented. The Act on the Implementation of the EU Directive on Network and Information Security, which entered into force on 30 June 2017, further strengthens the BSI's supervisory and enforcement powers for KRITIS operators. However, the BSI will continue its participatory and cooperative approach it has pursued in the UP KRITIS for 10 years.

Reported incidents from critical infrastructures (Chapter 2.3.5) during this period under review underline the necessity of the new reporting obligation.

Linking IT Security Actors

At numerous interfaces, the BSI works as a central competence centre with external partners in order to ensure IT security at a high level. Such a holistic approach with competencies for the Federal and State Governments enables the full development of the opportunities of digitalisation. By expanding this communication – first started as a pilot project in 2017 – the BSI will widen awareness for this aspect.

At the same time, bilateral and European cooperation is being expanded – in prevention, detection and development of uniform standards and procedures.

Conclusion for the German IT Security Landscape

Many IT security incidents that came to light in 2016 and 2017 showed that all actors have to be aware of their responsibilities to ensure successful IT security. WannaCry was able to cause such severe damages because systems could not be patched sufficiently. The BSI advocates more transparency for users in this area as well as more responsibilities for companies.

To better support constitutional bodies, Federal Authorities and operators of critical infrastructures appearing on-site quickly, flexibly and appropriately when needed, the BSI will keep forwarding the expansion of "Mobile Incident Response Teams" (MIRTs) as intended by the implementation of the cyber security strategy and the NIS Guideline Implementation Act.

In order to be able to actively take on its tasks and responsibilities in not only a reactionary way, but also in prevention and detection – to "get ahead" of the facts in the face of the outlined rapid technological development – the predictive power of the BSI has to be expanded. On the one hand, it must remain a driver in the area of cryptography. On the other hand, it must be able to identify and evaluate all technological trends relevant to IT security in the sense of a "technology radar" by screening newly emerging technologies and monitoring prioritised ones at an early stage, to be able to quickly develop the required technology know-how and to use it in a targeted manner as a "thought leader."

The new BSI report clearly shows that IT security is necessary to achieve successful digitalisation. As the national cyber security authority, the BSI will keep facing this challenge head on. The approach to sharing

information as far as possible (“need to share”) is our basic belief. Joint social efforts will enable the continuous increase of the level of IT security in digitalisation in the future as well.

4 Glossary

Advanced Persistent Threats
Advanced persistent threats (APT) are targeted cyber attacks on select institutions and organisations in which attackers gain long-term access to a network and then spread the attack to additional systems. The attacks are characterised by a high level of resource deployment and considerable technical capability on the part of the attackers; the attacks are generally difficult to detect.

Attack Vector
An attack vector denotes the combination of attack routes and techniques through which the attackers gain access to IT systems.

Application / App
An application, or app for short, is a piece of user software. The term 'app' is often used in relation to applications used on smartphones or tablets.

Adware
Adware refers to programs that are financed by advertising. Malicious programs that generate advertising for their creators also fall under this category.

Bot / Botnet
A botnet is a collection of computers (systems) that have been attacked by a remotely controllable malware program ('bot'). The affected systems are controlled by the botnet operator by means of a command-and-control server (C&C server).

Blinding
Blinding is a procedure generally used to protect against side-channel attacks in cryptography. Blinding can help to disguise the secret key (or parts of it) during an encryption operation so that no information can be extracted in relation to this key. A random number is generally added to the secret value which does not influence the crypto operation, but protects the genuine key.

CERT-Bund
CERT-Bund (Computer Emergency Response Team of the Federal Government) is located within the BSI and functions as the central coordinating body for government authorities for both preventive and reactive measures in the event of security-related incidents affecting computer systems.

CERT / Computer Emergency Response Team
A computer emergency response team is made up of IT specialists. Many companies and institutions have by now established CERTs to handle defence against cyber attacks, respond to IT security incidents and implement preventive measures.

Cloud / Cloud Computing
Cloud computing denotes the provision, use and billing of IT services via a network, where these services are dynamically adapted to demand. These services are offered and used exclusively in accordance with defined technical interfaces and protocols. The range of services offered within cloud computing covers the entire range of information technology, including infrastructure (such as computing power and memory), platforms and software.

CVE Database
Aim of the Common Vulnerabilities and Exposures (CVE) database is the introduction of a standard naming convention for Vulnerabilities in computer systems. Each registered vulnerability receives a running Number to guarantee a unique identification of that vulnerability. The database is maintained by the non-profit organization MITRE and has established itself as a registry of public vulnerabilities.

DANE
DNS-based Authentication of Named Entities (DANE) is a protocol which allows certificates to be bound to DNS names. A typical case is the storage of a TLS certificate. A DNS entry with the name TLSA is generated for this purpose. DNSSEC is necessary in order to protect these entries from manipulation.

Digital Personality Protection
Digital personality protection is the protection of the activities of important personalities in the digital sphere. In addition to the protection of private e-mail inboxes, this also includes measures such as the verification of Twitter and Facebook accounts.

DNS
The Domain Name System (DNS) assigns the relevant IP addresses to the addresses and names used on the Internet, such as www.bsi.bund.de.

DNSSEC
DNSSEC is a security extension for the Domain Name System (DNS). Entries in the DNS can be cryptographically signed by means of DNSSEC. Manipulation of these entries is then easier to detect.

DOS / DDoS Attacks
Denial-of-service (DoS) attacks target the availability of services, websites, individual systems or whole networks. When these attacks are carried out simultaneously, they are referred to as a distributed DoS or DDoS attack (DDoS = distributed denial-of-service). DDoS attacks are often performed by a very large number of computers or servers.

Drive-by-Downloads / Drive-by-exploits
The term 'drive-by exploits' refers to the automated exploitation of security vulnerabilities on a PC. The act of viewing a website, without any further user interaction, is sufficient to open up a vulnerability in the web browser, additional browser programs (plug-ins) or the operating system which can then be exploited, thereby enabling malware to be installed on the PC unnoticed.

Exploit
An exploit is a method or program code that can be used to execute commands or functions that are not intended through a vulnerability in hardware or software components. Depending on the type of vulnerability, an exploit can, for example, crash a program, extend user privileges, or execute arbitrary program code.

Exploit-Kit
Exploit kits or 'exploit packs' are tools for cyber attacks that are placed on legitimate websites. A variety of exploits are used in an automated way to try to find vulnerabilities in the web browser or its plug-ins and exploit these for installing malware.

Firmware
Firmware denotes software that is embedded into electronic devices. Depending on the device, firmware can either have the functionality of, for example, a BIOS, an operating system or application software. Firmware is specifically adapted to the respective hardware and is not interchangeable.

Nonce
Nonce stands for 'number used only once' and in cryptography represents a unique number, i.e. a number which is only used once in a context. Nonces are often generated by means of a random number generator and then used, for example, for creating an electronic signature and deleted after so that the same number cannot be used again for a different electronic signature. Nonces are also necessary for establishing the TLS connection.

OpenSSL
OpenSSL is a free software library that implements encryption protocols such as Transport Layer Security (TLS).

Patch / Patch Management
A patch is a software package that software manufacturers use to resolve security vulnerabilities in their programs or to implement other improvements. Many programs offer an automated update function to make the installation of these updates easier. Patch management denotes the processes and procedures that enable an IT system to obtain, manage and install available patches as quickly as possible.

Padding
A patch is a software package that software manufacturers use to resolve security vulnerabilities in their programs or to implement other improvements. Many programs offer an automated update function to make the installation of these updates easier. Patch management denotes the processes and procedures that enable an IT system to obtain, manage and install available patches as quickly as possible.

Phishing
The term 'phishing' is a combination of the words 'password' and 'fishing,' i.e. 'fishing for passwords.' The denote when attackers attempt to extract the personal data of an Internet user via bogus websites, e-mails or messages in order to misuse this data for their purposes, generally at the expense of the victim.

Plug-in
A plug-in is an extra piece of software or a software module that can be integrated into a computer program to extend its functionality.

Ransomware
Ransomware is defined as malicious programs which restrict or prevent access to data and systems and only release these resources upon payment of ransom money. It involves an attack on the availability of a security target and constitutes a form of digital extortion.

Root Zone
The root zone is the top-level zone in the hierarchical Domain Name System (DNS):
. Root Zone
.de Top-Level Domain 'de'
.bund.de Domain of Federal Government

RPKI
The Resource Public Key Infrastructure is a certificate infrastructure specifically used for protecting Internet routing.

Sinkhole
Sinkholes are defined as computer systems to which queries from botnet-infected systems are diverted. Sinkhole systems are typically operated by security researchers for detecting botnet infections and informing users who are affected.

Social Engineering
In cyber attacks involving social engineering, criminals attempt to mislead their victims into voluntarily disclosing data, bypassing security measures or willingly installing malware on their own systems. Just as in the field of espionage, cyber criminals are adept at exploiting perceived human weaknesses, such as curiosity or fear, in order to gain access to sensitive data and information.

Spam
Spam is defined as unsolicited messages sent by e-mail or using other communication services to a large number of people in a non-targeted way. Harmless spam messages generally contain unsolicited advertising. However, spam frequently also comes with attachments containing malware, links to infected websites or is used for phishing attacks.

SSL/TLS
TLS stands for Transport Layer Security and is an encryption protocol for the secure transmission of data on the Internet. Its predecessor SSL (Secure Sockets Layer) is another such protocol.

TLSA
See DANE.

UP KRITIS
UP KRITIS (www.upkritis.de) is a public-private partnership between critical infrastructure providers, their professional associations and relevant government agencies.

Imprint

Published by
Federal Office for Information Security (BSI)

Source
Federal Office for Information Security (BSI)
Godesberger Allee 185–189
53175 Bonn

Email
bsi@bsi.bund.de

Telephone
+49 (0) 22899 9582-0

Telefax
+49 (0) 22899 9582-5400

Version
August 2017

Print
Druck- und Verlagshaus Zarbock, Frankfurt am Main

Layout
Fink & Fuchs AG

Content and editing
Federal Office for Information Security (BSI)

Image credits
all images: iStock.com/jm1366

Graphics
Federal Office for Information Security (BSI))

Item number
BSI-LB17/506e

This brochure is part of the BSI's public relations work.
It is distributed free of charge and is not intended for sale.

www.bsi.bund.de